

**BI-STATE DEVELOPMENT AGENCY
D/B/A**



Metro

METRO

CODE OF CONDUCT

TABLE OF CONTENTS

TABLE OF CONTENTS.....	i
CHIEF EXECUTIVE OFFICER ENDORSEMENT	1
PURPOSE:	2
SCOPE:.....	2
RESPONSIBILITY AND AUTHORITY:	2
CONFLICT OF INTEREST:.....	3
ACCEPTANCE OF GIFTS OR GRATUITIES:.....	4
CONFIDENTIALITY AND PRIVACY:	4
OUTSIDE EMPLOYMENT AND BUSINESS OPPORTUNITIES:	5
POLITICAL CONTRIBUTIONS:.....	5
DISCRIMINATION & HARASSMENT:.....	5
PROFESSIONALISM:.....	5
PROTECTION AND USE OF METRO ASSETS:.....	5
REPORTING ILLEGAL AND UNETHICAL BEHAVIOR:.....	6
IMPROPER INFLUENCE OF AUDITORS' CONDUCT:	6
CODE ENFORCEMENT:	6
ANNUAL AGREEMENT – CODE OF CONDUCT:	7

CHIEF EXECUTIVE OFFICER ENDORSEMENT

Delivering with integrity is one of Metro's most important values. We all work hard every day to deliver transit solutions that enable people everywhere to grow and thrive. That is our purpose, and it is important. It is equally important that the actions we take as we deliver on that purpose are transparent and honest. At Metro, delivering with integrity is not optional. Without exception, it is the way we operate as one of the nation's top transit agencies.

What does it mean to deliver with integrity? It means we contribute our time, technology, and know-how to improve the communities where we work and live. It means we are committed to helping our customers, and growing our business, in ways that benefit the environment and the region we serve. We demand high performance and high standards. It also means that in everything that the Agency does we operate legally and ethically, in accordance with applicable laws and regulations and with the letter and spirit of those laws and regulations. Our Code of Conduct includes our general ethical principles and provides guidance on how to follow Metro policies and adhere to our legal requirements.

If, at any time, you have questions about the law or Metro policies, or encounter circumstances that the Code does not specifically address, we have provided additional resources in the Policy and Procedure Manager (PPM) application on MetroWeb, our internal website, as well as in our employee handbooks. If you are still not sure, please ask your supervisor, the Director of Workforce Diversity, the Director of Corporate Compliance, or the General Counsel.

All of us at Metro have an obligation to protect our Agency's interests. If you see something that does not seem ethical or right, please speak up. It is your responsibility as a member of our award-winning team to conduct yourself with the highest level of integrity and to alert others if you have questions or concerns.

Thank you for following our Code, living our values, and fulfilling our purpose.

/SIGNED/

John M. Nations
President and CEO

PURPOSE:

The Code of Conduct strengthens Metro's ethical and professional environment by clearly articulating the Agency's core values.¹ These core values are:

- **Customer Focus:** We strive to not only meet but also exceed our customer's needs and expectations.
- **Safety & Security:** The safety and security of our customers, the public, and our employees is our most important priority.
- **Character:** We value and practice honesty, integrity, respect, courtesy, teamwork, trust, directness, accountability, being receptive to other viewpoints and are committed to the success of others and Metro.
- **Ethical Practices:** We adhere to our code of ethics and other Metro standards of conduct and behavior. We practice and enforce these standards throughout Metro and in all our dealings with the public.
- **Communication:** We are committed to providing clear and accurate information and for being transparent at all times.
- **Recognition of Employee Contributions:** We recognize our employees who create, innovate, consistently support the day-to-day business requirements, and contribute to the success of Metro.

SCOPE:

Metro's Code of Conduct applies to all employees regardless of employment status unless represented by a collective bargaining agreement, which has its own set of employee behavioral guidelines.

The Code of Conduct represents Metro's guiding principles only. It cannot anticipate all circumstances and situations that employees may encounter. Metro employees are still expected to exercise good judgment at all times.

RESPONSIBILITY AND AUTHORITY:

In accordance with the Metro Board of Commissioners Policy, Chapter 60, Metro Senior Management will annually review and update the Code of Conduct. Once revised, the Chief Executive Officer (CEO) will sign it.

¹ Although this Code is intended to provide guidance for all Metro employees, it is understood that the conduct of represented employees is governed by their collective bargaining agreement and operating rules.

All members of management will receive Code of Conduct training and are then responsible for training, implementing, and enforcing the Employee Code of Conduct with their employees, in consultation with the Human Resources Department and the Director of Corporate Compliance.

Each year, Metro employees must read, understand, and sign the Code's agreement shown on the last page. The behavior of our employees reflects on the Agency for better or for worse. For that reason, all employees are expected to behave in accordance with the Code of Conduct. An employee's conduct at work, when serving as a Metro Ambassador or otherwise representing Metro in the community, or even in his/her private life that reflects negatively on the Agency may subject the employee to discipline up to and including termination.

If an employee becomes aware of a serious breach of this Code of Conduct, the employee has a responsibility to report that breach to her/his supervisor and to the Director of Corporate Compliance. Any employee who reports a breach in good faith is protected from reprisal for doing so, even if the reported breach is not confirmed through investigation. If an employee feels uncomfortable reporting a breach to her/his supervisor, or if she/he feels the issue has not been adequately addressed, then the employee is encouraged to report it using Metro's Compliance and Fraud Helpline service at EthicsPoint Inc. Reports can be made toll-free at 1-85-LINK2HLP (1-855-465-2457) or at www.ethicspoint.com. All reports to EthicsPoint are completely confidential.

All questions regarding the scope, interpretation or application of the Employee Code of Conduct should be referred to the Director of Workforce Diversity, the Director of Corporate Compliance, or the General Counsel.

COMPLIANCE WITH LAWS, RULES, AND REGULATIONS:

Obeying the law, both in letter and in spirit, is one of the key elements on which Metro's ethical and professional standards are built. All employees and officers must respect and obey the laws and regulations of the cities, counties, and states in which we operate, as well as with the requirements of federal law.

CONFLICT OF INTEREST:

Conflicts of interest are prohibited as a matter of Metro policy. A "conflict of interest" exists when a person's private interest interferes, or even appears to interfere, in any way with the interests of Metro. A conflict of interest will be deemed to exist without limitation, in situations or transactions wherein an employee:

- Has an outside interest that materially encroaches on time or attention, which should be devoted to Metro's affairs;

- Has a direct or indirect interest in or relationship with an outsider that is or that might be implied or construed to be inherently unethical or that make possible personal gain to the employee, renders the employee partial toward the outsider for personal reasons or otherwise inhibits the impartiality of the employee's business judgment, places the employee of Metro in an equivocal, embarrassing, or ethically questionable position, or reflects on the integrity of Metro;
- Takes personal advantage or benefits personally from an opportunity, which properly belongs to Metro, or;
- Uses Metro property for personal gain.

Employees who are subject to the Code of Conduct are required to read and annually sign a Conflict of Interest Statement.

ACCEPTANCE OF GIFTS OR GRATUITIES:

Metro employees may not solicit gifts, gratuities, favors, or anything of monetary value from contractors, potential contractors, or parties to subcontracts. Employees may accept occasional unsolicited gifts of nominal value, but may never accept gifts of cash or cash equivalents, such as gift cards, nor should any gifts be accepted from a potential bidder to a current or near imminent Metro procurement. All business meals and entertainment must be customary, unsolicited, and infrequent, in good taste, reasonable and customary in value, and provided for legitimate business reasons. If the provider of the meal or entertainment is not in attendance, or is a potential bidder to a current or near imminent Metro procurement, the event is not for a legitimate business purpose. It should then be considered a gift and can only be of nominal value. Employees must politely decline entertainment or gifts that do not comply with this Code. Employees who are uncertain about how to handle a particular situation regarding a gift that has been offered to him/her should consult a supervisor or contact the Director of Corporate Compliance for guidance.

CONFIDENTIALITY AND PRIVACY:

Employees may access privileged and confidential information, whether they are already authorized to access it or they accidentally or inadvertently access unauthorized confidential information. It is every employee's duty to protect the confidentiality of all such information and to report any incidents of unauthorized access to their supervisor as soon as possible.

OUTSIDE EMPLOYMENT AND BUSINESS OPPORTUNITIES:

Employees can seek additional employment outside of Metro as long it does not conflict with the employee's performance of their Metro job duties and responsibilities. Employees must notify their supervisor in writing of the nature and conditions of any outside employment that they hold or expect to hold.

Employees and officers are prohibited from realizing personal gain for themselves using Metro's property, information, or sources without the consent of the Board of Commissioners.

POLITICAL CONTRIBUTIONS:

Do not use Metro funds or assets, including facilities, equipment, or trademarks in connection with your personal political activities or interests. Employees must use care not to give the impression that Metro supports or endorses any candidate, campaign, or issue with which he/she is personally involved.

Before engaging in any activity on behalf of Metro that might be considered a political contribution or lobbying, obtain written approval from the Office of Government Affairs.

DISCRIMINATION & HARASSMENT:

Metro is firmly committed to providing equal opportunity in all aspects of employment and will not tolerate any discrimination or harassment based on race, color, religion, sex, national origin or any other protected class. Employees are expected to fully support and conduct themselves in a manner consistent with Metro's commitment to equal opportunity.

PROFESSIONALISM:

Dealing with our customers, co-workers, management, vendors, consultants, and other external entities requires all employees to use the utmost care, patience, and integrity in order to ensure that the highest level of communications and professional interactions are maintained at all times.

PROTECTION AND USE OF METRO ASSETS:

All employees and officers must protect Metro's physical assets (e.g., vehicles, equipment, tools, supplies, computer workstations, and facilities), electronic assets (network logins, passwords, access to applications and data), as well as ensure their efficient and protected use. All Metro assets must be used for legitimate Metro business purposes only. Employees who become aware of any suspected incident of illegitimate use, illegal use, fraud, or theft should first report it immediately to their supervisor, or to the EthicsPoint Compliance and Fraud Helpline, for investigation.

REPORTING ILLEGAL AND UNETHICAL BEHAVIOR:

Employees are encouraged to not take matters into their own hands and to talk to supervisors, managers, or other appropriate personnel about observed behavior that they believe may be illegal or a violation of the Code of Conduct. To report any case or suspicion of illegal or unethical behavior, fraud, or corruption, please call the Compliance and Fraud Helpline at 1-85-LINK2HLP (1-855-465-2457) or login at www.ethicspoint.com. Employees who make a good faith report of suspected misconduct by others will not be retaliated against in any manner. When employees do report such incidents, however, they are expected to fully cooperate with any investigation of the reported misconduct.

IMPROPER INFLUENCE OF AUDITORS' CONDUCT:

It is prohibited to take any direct or indirect action to coerce, manipulate, mislead, or fraudulently influence Metro's independent auditors to intentionally render Metro's financial statements materially misleading.

Metro's policy is to comply with all financial reporting and accounting regulations applicable to Metro. If any employee or officer has concerns or complaints regarding accounting or auditing matters, then he or she is encouraged to contact the Director of Corporate Compliance and the Director of Internal Audit.

CODE ENFORCEMENT:

All officers and employees are required to comply with this Code. Anyone who is found to have violated it may be subject to disciplinary action, up to, and including, termination of employment.

ANNUAL AGREEMENT – CODE OF CONDUCT:

To help ensure compliance with the Code of Conduct, Metro requires that all officers and employees not covered by a collective bargaining agreement review the Code of Conduct and acknowledge their understanding and adherence in writing on an annual basis.

AGREEMENT:

I have read and understand the Code of Conduct. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to Metro policy and/or applicable law.

Please note: Employees who are able to access the Code of Conduct through Metro’s electronic Policy and Procedure Manager (PPM) system can complete their annual agreement electronically. Otherwise, please print the annual acknowledgement page, sign it, and provide the original copy to their supervisor.

Employee Name

Employee Signature

Date

Security Awareness Slogans, Mottos, Tag lines, Catch Phrases, Maxims...

- Control + Alt + Delete
When You Leave Your Seat
- Before leaving the scene, clear your desk and your screen.
- If something sounds too good to be true... there's probably a scammer behind it.
- Leave a clear desk while you're away and at the end of each day.
- Give your computer a rest when you're not at your desk.
- Don't get hooked by phishers.
- Phishing: If you suspect deceit, hit delete!
- There's no excuse for computer misuse.
- Prepare for Disaster: Recover Faster.
- SEC_RITY is not complete without U!
- Sec-UR-rity - You are at the center.
- Amateurs hack systems, professionals hack people.
- Think before you click.
- Protect personal information. The identity saved could be your own.
- Don't let your trash become someone else's treasure. Feed your shredder often.
- Passwords: Longer is Stronger.
- You wouldn't share your ATM pin, so why would you share your password?

- If you suspect deceit, hit DELETE.
- Passwords are like dirty socks. If left lying around, they'll create a stinky mess.
- The bug stops here. Use anti-malware programs to prevent virus infections.
- Security by Obscurity. Don't leave data or portable computing devices alone and in view.
- You can't un-ring a bell. Before you give PII* to anyone, make sure that access is allowed.
(* PII stands for Personally Identifiable Information)
- We all value privacy. Report actual or suspected spills of PII... before they become floods.
- Because we care, we're security aware.
- Report data spills before molehills become mountains or small leaks become fountains.
- Before sharing PII, know whom, what, and why.
- Good security increases shareholder value.
- Don't be shy about protecting PII.
- Know how and when to say no. Don't share protected personal information with strangers.
- Don't be afraid to say no.
- To show our respect, we protect personal information that we collect.
- Protecting PII is everyone's job; PII is not everyone's business.
- Stop Neglect. Protect before you connect.

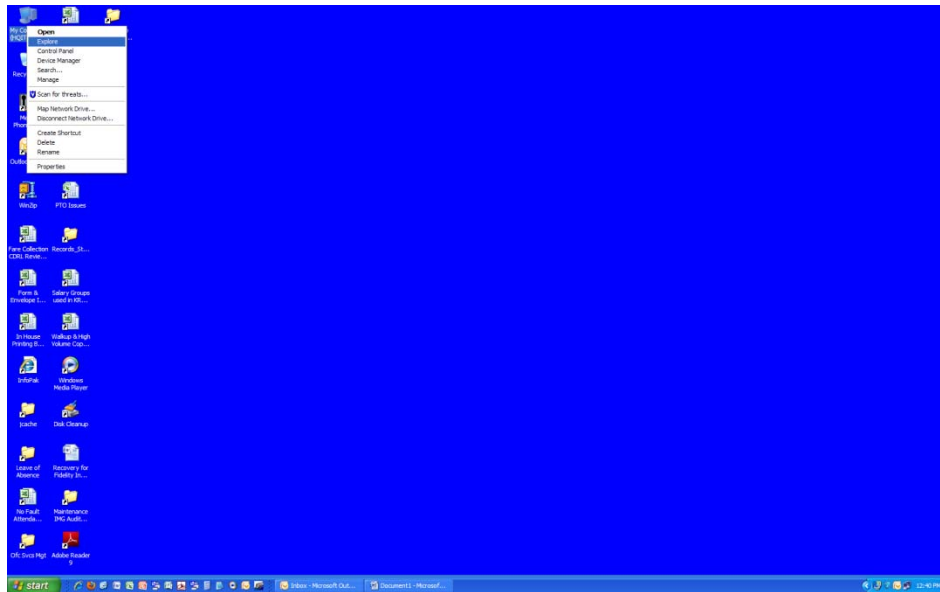
More Slogans

- A check that does not bounce is called the Security Check. Do it every day before you leave!
- Do Your Part - Be Security Smart!
- Don't be Quick to Click... be wary when you shop online.
- Restart is Smart!
(When leaving your computer for the day, always choose restart. This allows your computer to receive updates from the IT department through the network.)
- A user who restarts is a user after my own heart! - Valentine
- Your CAC Card - Don't leave the office without it!
- Passwords are like toothbrushes. They are best when new and should never be shared.
- When you and your system part away, your system should be first off for the day.
- Your mind is a storage room of information, keep the door locked.

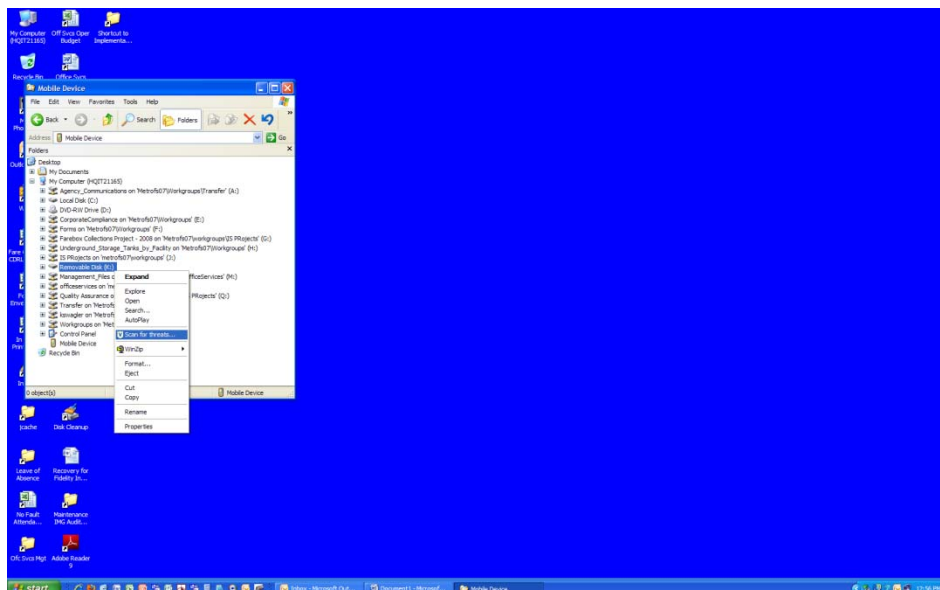
How to Scan Removable Media for Viruses

Virus scans can be done several ways when you insert a flash drive, CD, or DVD into your system:

- If you copy a file from your disk or flash drive to your system or to a network folder, the file is automatically scanned for viruses;
- If you open a file from your disk or flash drive, the file is automatically scanned for viruses; or
- You can also scan the entire disk or flash drive by:
 - Right-clicking on your **My Computer** icon and select **Explore**



- Right-click on your CD/DVD drive or your Removable Disk drive and select **Scan for threats...**

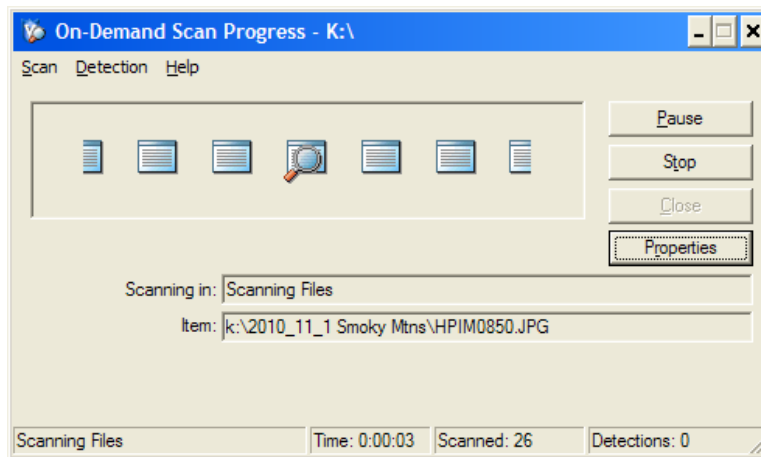


How to Scan Removable Media for Viruses

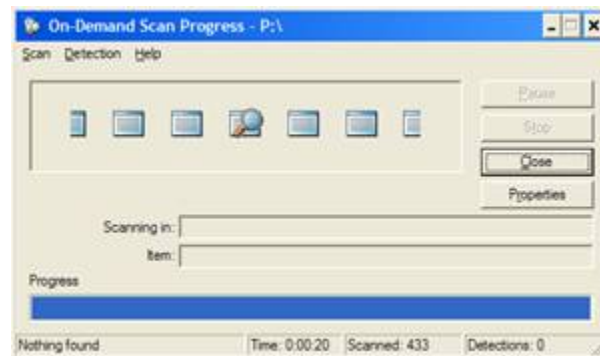
- Click the **Clean** button



- The scan is done on the selected media



- If anything is found, you can select the options to remove it. When the removal is completed, or if nothing is found, click the **Close** button.



Safe Computing Guide

Question #1

Do I trust the computer I am using?

- Patched/Updated
- Anti-Virus
- Firewall



Yes

Question #2

Do I trust the site I am accessing?

- Is it reputable?
- HTTPS
- Is it certified?



Yes

Question #3

Do I trust the network?

- Encrypted (WPA2)
- Is access restricted to the public?
- Who else is on the network?



Yes



You are safe to browse the Internet

Unsure

You may not be safe

Follow these guidelines to reduce your risk

- Avoid entering confidential information until you have a more secure network connection.
- Read, understand, and heed ALL browser warnings you see (i.e. pop-ups.)
- Beware of unusual computer behavior- operating extremely slowly (indication of snooping).
- Consider alternative connections such as a cell phone.

No

No

No

You are not safe

You could lose:

My money in the bank
Access to change student grades
Access to purchase with P-card
Access to PeopleSoft

SSN #'s including your own
Cal Poly's reputation and your own
Your bank accounts and credit cards
Your identity



**BI-STATE DEVELOPMENT AGENCY
D/B/A**



Metro

***METRO
INFORMATION SECURITY POLICY***

Table of Contents

1. Background	1
2. Purpose	1
3. Roles and Responsibilities	2
3.1. Metro Computer Users:	2
3.2. Executive Staff	3
3.3. Division Information Security Managers (at least one per division).....	3
3.4. Metro Information Security Officer:	4
3.5. Vice President & CIO:	5
3.6. IT Information Security Manager:	5
3.7. IT System/Network Administrators or Technical Contacts:.....	6
3.8. Computer Emergency Response Team (CERT):.....	7
4. Data Classification	7
5. Access Control	9
6. Virus Prevention	10
7. Intrusion Detection.....	11
8. Internet Security	11
9. System Security	11
10. Acceptable Use Policy.....	12
11. Exceptions.....	12
12. Incident Response & Reporting.....	13
13. Other IT Policies.....	13
14. Waiver Procedures	13
15. Eligibility.....	14
16. Document(s)/Supplement(s).....	14
17. Regulatory Requirements.....	14
18. Related Board Policies	14
19. Definition of Terms.....	14

Policy Number: Original # IT-07-03 (Version 1)
Approval Date: July 13, 2007
Effective Date: July 13, 2007
Last Revision: July 25, 2007
Responsible Executive(s): Vice President & Chief Information Officer (CIO), Director of Corporate Compliance
Process Owner(s): Corporate Compliance, Information Technology (IT), and Human Resources

1. Background

All Metro divisions and functions are highly dependent upon the Agency's Information Technology (IT) infrastructure to support business activities and to provide services, both internally and externally. This infrastructure is comprised of the Agency-wide computer and data communications network, together with all of the enterprise and division computer systems, devices, and applications that use the network. Because Metro is dependent on these IT assets, Metro employees must understand their roles and their responsibility for Information Security so they can carefully protect these assets from all sources of harm and from potentially significant service disruptions or failures.

2. Purpose

Commitment and teamwork among all employees are necessary to ensure Information Security, and all employees share responsibility for ensuring Information Security. This policy provides a framework for that cooperation and defines the roles and responsibilities of Metro employees and divisions. Its purpose is to outline the measures necessary to ensure that risks to IT assets are effectively identified; appropriate security measures and controls are in place; and appropriate steps will be taken in response to Information Security-related incidents.

It is intended to accomplish the following Information Security objectives:

- Prevent loss of Metro's information assets
- Ensure the security, confidentiality, integrity, and availability of electronic data
- Prevent unauthorized access to Metro's IT infrastructure and the business systems it supports
- Ensure continuity and reliability of technology infrastructure, including business support systems and communication networks

3. Roles and Responsibilities

3.1. Metro Computer Users:

All Metro employees, contractors, and other authorized computer users with access to Metro's IT infrastructure are responsible for the following:

- Comply with IT policies and standards for the use of computer systems and network resources.
- Safeguard computerized data (i.e. volumes, directories, and files) to which access has been granted in accordance with rights and permissions granted by the division owning the data.
- Safeguard computer equipment and prevent unauthorized access to computerized information, computer business systems, or the network. This includes taking reasonable precautions to protect and maintain personal passwords and to prevent unauthorized use of computers, accounts, software programs, or computerized data by others.
- Report all security incidents, such as breaches of data or network security or compromises of computer or network resources, to his/her supervisor, the Division Information Security Manager, and the Metro Help Desk when the employee becomes aware of such incidents.
- Do not attempt to disable enterprise virus scanning, spyware, and spam protection software on any Metro workstation.
- Scan all removable media [diskettes, CD's, DVD's, removable hard drives and flash memory, digital cameras and their associated flash memory, etc.] for viruses before they are used. This can be done by inserting the removable media and running a virus scan on the media.
- Do not attempt to eradicate viruses without IT assistance.
- When virus infection is suspected, immediately stop using the workstation, log off from all networks, and notify the Metro Help Desk.
- Do not leave a workstation or terminal unattended without first activating an IT-provided password-protected screen-saver, a password-supported workstation-locking program, or logging out.
- If unauthorized persons are in a position to see the workstation screen when sensitive data is displayed, invoke an IT-provided password-protected screen-saver, a password-supported workstation-locking program, or log out.
- Do not connect any device that was not procured and installed by Metro IT support staff, including personal computers, printers, cellular phones, iPads, or any networking equipment to the network without first obtaining written approval by the division manager and the Vice President and CIO. Once approved, IT staff will perform all connections.

- Be personally responsible and accountable for all activities performed at his/her Metro workstation or terminal, in accordance with the permissions granted through his/her User ID and passwords.
- A User ID is restricted to the person to whom it is assigned. Do not use another person's User ID or allow another person to use your User ID.
- When creating passwords, use at least eight alphanumeric characters and avoid use of words or combinations of characters or numbers that are not unique, or that can be guessed, surmised, calculated, inferred, or predicted by others.
- Use caution upon receiving email attachments from unknown senders. Email attachments can be virus infected and exercising skeptical treatment of email attachments will help mitigate mass email virus outbreaks. When in doubt, delete the message, empty the email wastebasket immediately, and notify the IT Help Desk.
- Provide electronic or written acknowledgement that you have received, have read, and will comply with IT Information Security standards.

3.2. Executive Staff

All Metro Executive Staff are responsible for assigning an employee to serve as their Division's Information Security Manager. This individual will be responsible for Information Security compliance.

3.3. Division Information Security Managers (at least one per division)

There must be at least one Information Security Manager per division whose responsibilities include:

- Acting as a liaison with the Director of Corporate Compliance (assigned as Metro's Information Security Officer) to ensure Information Security measures and precautions are implemented in their division.
- Serving as their division's primary contact for Information Security related issues and incidents.
- Working with the Director of Corporate Compliance to:
 - Educate all division employees to contact the Metro Help Desk (314-982-1400 ext 5555) at any time (24 hours a day, 7 days a week) whenever Information Security-related incident impacts division operations.
 - Ensure that all division employees are held accountable for adhering to the Information Security policy just as they would for other job related function by obtaining written acknowledgement from all division employees that they have received, read, and will comply with Information Security standards.

- Notify division employees of all changes or updates to Information Security standards.
- Ensure that non-employee personnel (e.g. contractors, volunteers, etc.) authorized to access Metro IT assets comply with this policy and Information Security standards through inclusion of specific, standardized language in their contracts or agreements. This must be reviewed and approved by the Vice President, Procurement and Inventory Management.
- Provide periodic and timely feedback to IT and the Director of Corporate Compliance regarding division adherence to Information Security standards and responses to Information Security threats or incidents. This feedback can be accomplished as part of previously scheduled internal or external audits or compliance reviews.

• **The Human Resources Division Information Security Manager(s) has the following additional responsibilities:**

- Conducting initial Information Security awareness training for all new employees to ensure they understand and adhere to Information Security policies and standards.
- Obtaining electronic or written acknowledgement from all new employees that they have received, read, and will comply with Information Security standards.

3.4. Metro Information Security Officer:

The Director of Corporate Compliance serves as the Metro Information Security Officer and is responsible for the following:

- Reviewing the Metro-wide Information Security program to ensure the IT infrastructure possesses a level of security commensurate with the risk and magnitude of the harm that could potentially result from the loss, misuse, disclosure, or modification of electronic information.
- Conduct annual Information Security awareness refresher training to ensure all Metro employees understand and adhere to Information Security policies and standards.
- Working with the Vice President & CIO to:
 - Establish and maintain Metro-wide Information Security policies and standards through an enterprise Information Security management program.
 - Approve content of Information Security email communications before Metro-wide dissemination.
 - Determine the root causes for any Information Security breach and implement measures to reduce the likelihood of reoccurrence.

3.5. Vice President & CIO:

The Vice President & CIO is responsible for the following:

- Implement a Metro-wide Information Security program to ensure the IT infrastructure possesses a level of security commensurate with the risk and magnitude of the harm that could potentially result from the loss, misuse, disclosure, or modification of electronic information.
- Work with the Director of Corporate Compliance to establish and maintain Metro-wide Information Security policies and standards through an enterprise Information Security management program.
- Appoint an employee as IT Information Security Manager to be responsible for maintaining an Information Security strategy and related standards consistent with changing technology and threats to the IT infrastructure.
- Approve content of Information Security email communications before Metro-wide dissemination.
- In the event of an Information Security breach, determine the resulting loss, if any, and inform the Director of Corporate Compliance. The Risk Management Department, other Agency departments, or law enforcement authorities may be contacted when warranted by this review.

3.6. IT Information Security Manager:

The IT Information Security Manager is assigned by the Vice President & CIO and is responsible for the following:

- Provide email virus protection for all email received from the Internet and enterprise support for all email security related issues.
- Disseminate approved Information Security email messages, including, but not limited to, virus infections and hacker intrusions.
- On an ongoing basis, identify, update, and maintain information regarding potential security vulnerabilities, risks, and threats to the enterprise IT infrastructure; and distribute Information Security information to appropriate staff.
- Provide instructions and coordination regarding software configuration standards for servers and desktop systems that are or may be attached to the enterprise network where necessary to ensure Information Security.
- Periodically review and update Information Security standards and guidelines based upon IT industry best practices that are necessary to contribute to a Metro-wide scalable, interoperable, and secure operating environment.
- Establish and maintain procedures for software change and patch management to provide a secure computing environment.

- Establish procedures for virus protection updates to provide a secure computing environment.
- Monitor for security alerts from IT organizations, and patch releases for major operating systems and application software environments, and escalate when appropriate to the Vice President & CIO for further action.
- Coordinate and manage the response to all enterprise-level, Information Security-related incidents or events including, but not limited to, virus infection and hacker intrusions. Notify the Vice President & CIO of incident progress in a timely manner.
- Inform the Vice President & CIO and the Chief Financial Officer (CFO) of all attempted breaches or intrusions of any Metro information system, application, database, or data storage media containing Metro financial data including:
 - Credit cards/banking transactions
 - Cash management
 - Any financial reporting matter, including any web page addresses where the breach and the breached information are located.
- Inform the Vice President & CIO and the Vice President of Human Relations (HR) of all attempted breaches or intrusions of any Metro information system, application, database, or data storage media containing Metro employee data including:
 - Social Security numbers, addresses and other employee identification and contact information
 - Employee Protected Health Information (PHI)
 - Any HR reporting matter, including any web page addresses where the breach and the breached information are located.
- Document and track all Information Security events to closure.
- Establish a means for contacting the IT Computer Emergency Response Team (CERT) members and technical staff for IT security compliance, 24 hours a day, 7 days a week, in the event of an Information Security-related incident that impacts department or Metro operations.
- Prepare division compliance reports for Information Security standards to the Vice President & CIO for distribution to Metro division heads and Information Security liaisons.

3.7. IT System/Network Administrators or Technical Contacts:

System/Network Administrators or technical contacts are assigned by the IT Division to perform daily monitoring and maintenance for all components of the enterprise IT

infrastructure. They are specifically responsible for the following functions related to Information Security:

- Configure and manage all computer information systems and network devices in accordance with Metro Information Security policies and standards.
- Routinely maintain Metro computer information systems (e.g. servers, personal computers, laptop computers, printers, iPads, etc.), including system administration and management for division business systems, as necessary to ensure secure operation.
- Establish technical mechanisms that permit IT management to monitor and confirm compliance of computer system, network device configuration, and network security policy settings.
- Maintain user rights and password policies for all computerized business systems as necessary to ensure authorized access is limited to individuals who require access to applicable systems to perform Metro business.
- Apply patch management changes in accordance with the IT Production Control Policy and Procedures and include change management request submissions to the appropriate system patch management coordinators.
- Report Information Security incidents and potential threats, which could potentially compromise the enterprise network, to IT management and the Metro Director of Corporate Compliance.

3.8. Computer Emergency Response Team (CERT):

The CERT provides accelerated problem notification, damage control, and problem correction services in the event of a declared computer-related enterprise emergency. Emergencies include, but are not limited to, virus infection and hacker intrusions. CERT members must include:

- Vice President & CIO
- Director of Corporate Compliance
- IT Senior Management and other IT technical sections as appropriate for the incident
- Divisions or departments outside of IT that may be directly involved in the CERT team such as Risk Management, Safety, Communications, and others as needed

4. Data Classification

4.1. It is essential that all Metro data be protected. There are, however, data sensitivity/criticality gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. The three data classifications in use are:

- High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislations, such as Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or the Data Protection Act is in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements.

This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to Metro services if disclosed or modified. The Metro data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

- Confidential - Data that would not expose Metro to loss if disclosed, but that the Metro data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.
- Public - Information that may be freely disseminated.

- 4.2. All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the Agency.
- 4.3. Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.
- 4.4. No Metro-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- 4.5. Data custodians are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.
- 4.6. High-risk data must be encrypted during transmission over unsecured channels. This includes wireless and mobile devices.
- 4.7. Confidential data should be encrypted during transmission over unsecured channels.
- 4.8. All appropriate data should be backed up, and the backups tested periodically as part of a documented, regular process.
- 4.9. Data backups must be handled with the same security precautions as the data itself. When systems are disposed or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

5. Access Control

- 5.1. Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and proactively managed.
- 5.2. Where possible and financially feasible, more than one person must have full rights to any Metro-owned server storing or transmitting high-risk data.
- 5.3. Access to the network, servers, and application systems should be provided by individual and unique logins, and must require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
- 5.4. Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. When limited access to Metro-related documents or files is required specifically and solely for the proper operation of Metro divisions, and where available technical alternatives are not feasible, exceptions are allowed under an articulated division policy that is available to all affected division personnel. Each such policy must be reviewed by the division Executive Officer, and then submitted to the Vice President & CIO and the Director of Corporate Compliance for approval. All users must secure their username or account, password, and system access from unauthorized use.
- 5.5. All users of systems that contain high risk or confidential data must have strong passwords (i.e. one that is difficult to guess or hack) of:
 - At least eight alphanumeric characters (both letters and numbers)
 - At least one upper and lower case letter
 - At least one special character or symbol (@, #, \$, %, etc.), if allowed by the application

Empowered accounts, such as system administrator, root, or supervisor accounts, must be changed immediately after the assigned employee leaves Metro.
- 5.6. Only temporary user ID passwords can be placed in email messages.
- 5.7. Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- 5.8. Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- 5.9. Users are responsible for safe handling and storage of all Metro authentication devices. Authentication tokens (such as a Secure ID card) should not be stored with a computer

that will be used to access Metro network or system resources. If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing division so that the device can be disabled.

- 5.10. Terminated employees must have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, user access reviews should be conducted by the division Information Security Manager at least semi-annually.
- 5.11. Transferred employee access, as well as the employee(s) who now assumed the transferred employees responsibilities, must be reviewed and adjusted within the first two weeks after transfer.
- 5.12. Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons, and date and time of logon and logoff.
- 5.13. Activities performed as System Administrator, Database Administrator, or super-user must be recorded in read-only system logs as much as possible.
- 5.14. Personnel who have system or database administrative access should use other less powerful accounts for performing non-administrative tasks, such as simple database queries, checking email, editing Microsoft Office documents, and so on. Procedures for reviewing system logs must be documented and approved by the Vice President & CIO and the Director of Corporate Compliance.
- 5.15. Outside access to systems: The Procurement and Inventory Management Division authorizes outside vendors access to Metro's procurement system so they may respond electronically Procurement's proposal, quotation, or other business requests. Each access must be approved and regularly monitored by Procurement and IT.

Vendors performing IT technical support functions, such as software upgrades or resolving technical issues, should be temporary. Each access must be approved and regularly monitored by IT.

6. Virus Prevention

- 6.1. The willful introduction of computer viruses or disruptive/destructive programs into the Metro IT environment is prohibited, and violators are subject to prosecution under applicable law. If such introduction of computer viruses or disruptive/destructive programs into the Metro IT environment is done by a Metro employee, the employee is subject to discipline, up to and including termination of employment, as well as being subject to prosecution under applicable law.
- 6.2. All desktop systems that connect to the network must be protected with an approved and licensed anti-virus software product that it is kept updated according to the vendor's recommendations.

- 6.3. All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- 6.4. The email server must scan headers of all incoming data including electronic mail for viruses. Outgoing electronic mail should be scanned where such capabilities exist.
- 6.5. Where feasible, system or network administrators should inform users when a virus has been detected. This can be done through email and postings on MetroWeb whenever possible. If the virus is within the email system, alternate means of communication, (phone, radio, paper memos) must be used.
- 6.6. Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

7. Intrusion Detection

- 7.1. Intruder detection must be implemented on all servers and workstations containing data classified as high risk.
- 7.2. Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- 7.3. Server, firewall, and critical system logs should be reviewed frequently by the IT Information Security Manager, the Vice President & CIO, and the Director of Corporate Compliance. Where possible, automated review must be enabled and alerts must be transmitted to the administrator when a serious security intrusion is detected.
- 7.4. Intrusion tools should be installed where appropriate and checked on a regular basis.

8. Internet Security

All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk or confidential.

9. System Security

All systems connected to the Internet must have a vendor-supported version of the operating system installed.

All systems connected to the Internet must be current with security patches.

System integrity checks of host and server systems housing high-risk Metro data should be performed.

10. Acceptable Use Policy

Metro's policy on appropriate and acceptable use for Metro's Information Systems is as follows:

- 10.1. Metro computer resources must be used in a manner that complies with Metro policies, state and federal laws and regulations. It is against Metro policy to install or run software requiring a license on any Metro server, workstation, cellular phone, or smart device without a valid license.
- 10.2. Use of Metro's computing and networking infrastructure by Metro employees unrelated to their positions must be limited in both time and resources and must not interfere in any way with Metro functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.
- 10.3. Uses that interfere with the proper functioning or the ability of others to make use of Metro's networks, computer systems, applications, and data resources are not permitted.
- 10.4. Use of Metro computer resources for personal profit is not permitted.
- 10.5. Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations. The use of network sniffers is restricted to IT system administrators who must use such tools to solve network problems. Auditors or security officers in the performance of their duties may also use them. They must not be used to monitor or track any individual's network activity except under special authorization as defined by Metro policy that protects the privacy of information in electronic form.

Please forward any recommended changes to this Use Policy to the Vice President & CIO and the Director of Corporate Compliance.

11. Exceptions

In certain cases, compliance with specific Information Security policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- 11.1. Required commercial or other software in use is currently unable to support the required Information Security features.
- 11.2. Legacy systems in use that do not comply; however, compliant systems are approved and scheduled to replace the legacy systems within a 12 to 18-month period.
- 11.3. Costs for reasonable Information Security compliance are disproportionate relative to the probability, risk, and potential damage from an associated security breach.

In such cases, divisions must submit a written explanation of the Information Security compliance issue and a plan for coming into compliance with this Information Security Policy in a reasonable amount of time. Explanations and plans must be submitted for approval by the Vice President & CIO and the Director of Corporate Compliance.

12. Incident Response & Reporting

The IT Information Security Manager will use the following procedures in the event of an enterprise-level Information Security issue, (i.e., virus, worm, denial of service attack, etc.):

- 12.1. Serve as the "Situation Lead" and coordinate all problem resolution efforts.
- 12.2. Assemble the CERT Team, other IT technical sections, and other division Information Security Managers as appropriate for the incident.
- 12.3. Receive regular status updates from the CERT team as the central point of contact for the situation.
- 12.4. Ensure that emerging and hourly update information is provided to IT senior management, the CERT team, and other division Information Security Managers.
- 12.5. De-escalate and close out incidents when resolved.

13. Other IT Policies

In addition to the policies and procedures outlined herein, Metro employees will abide by all IT standards pertaining to Information Security. These standards may be updated from time to time because of changing IT systems and security requirements. Additional Information Security standards may also be established, and accordingly, those standards must be followed to protect Metro's enterprise IT infrastructure. The following is a list of security standards that have been established as of the publication date of this administrative regulation. Copies are available in Metro's Policy and Procedure Manager (PPM) system.

14. Waiver Procedures

Before any division can operate outside this regulation and established IT Information Security standards, the Division Executive must submit a waiver request stating the specific information standards to be waived to the Vice President & CIO and the Director of Corporate Compliance for review and approval. Waivers will not be approved unless they meet all requirements to protect Metro's infrastructure. The request must include the following:

- Description of the Information Security waiver request
- Statements clearly explaining the business justification for operating outside of this regulation or Information Security standards

- Description of this policy's provisions that will not be met
- Assessment of the security risk potential for not complying with this regulation
- Alternative security measures that will be taken by the division to ensure the security for both the affected information systems and Metro's enterprise IT infrastructure are maintained.

15. Eligibility

This policy applies to all Metro employees, contractors, and volunteers.

16. Document(s)/Supplement(s)

N/A

17. Regulatory Requirements

Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541; 815 ILCS 530/Personal Information Protection Act; Missouri Personal Information Data Privacy Notification and Encryption Laws: Section 407.1500

18. Related Board Policies

N/A

19. Definition of Terms

19.1. **Authorized User:** A Metro employee or contractor who has been granted authorization by the IT Information Security Manager, or his or her designee, to access an Electronic Information Resource and who invokes or accesses an Electronic Information Resource for performing his or her job duties or other functions directly related to his or her affiliation with Metro. The authorization granted is for a specific level of access to the Electronic Information Resource as designated by the Electronic Information Resource Manager, unless otherwise defined by Metro policy. An example of an Authorized User includes someone who handles business transactions and performs data entry into a business application, or someone who gathers information from an application or data source for the purposes of analysis and management reporting.

19.2. **Computer Virus:** An example of Intrusive Computer Software (see definition below).

19.3. **Electronic Information Resource:** An information resource that is maintained in electronic, or computerized format, and may be accessed, searched and retrieved via electronic networks or other electronic data processing technologies (e.g., CD-ROM, DVD, flash drive, etc.)

19.4. **Intrusive Computer Software:** Intrusive computer software (such as a computer virus) is an unauthorized program designed to embed copies of itself in other programs, to modify programs or data, or to self-replicate. Intrusive computer software may be spread via removable storage media or via a network. The term "intrusive computer software" as it is used in this policy, is intended to encompass the variety of such unauthorized programs, including viruses, bacteria, worms, Trojan Horses, etc.

19.5. **IT Information Security Manager:** The individual assigned by the Vice President & CIO to have oversight responsibility for Agency Information Security programs. Although responsibility for compliance with this policy will most likely rest with a number of Metro employees, the IT Information Security Manager must facilitate Metro compliance with this policy through collaborative relationships with Metro management.

19.6. **Security:** Measures taken to reduce the risk of:

- Unauthorized access to or modification of Electronic Information Resources, via logical, physical, or managerial means
- Damage to or loss of Electronic Information Resources through any type of disaster (such as employee error or other accidents, long-term system failures, natural disasters, and criminal or malicious action).

Security also encompasses measures taken to reduce the impact of any violation of security or a disaster that occurs despite preventive measures.

19.7. **Server:** A multi-user computer, including mainframes, servers, and personal computers providing services to multiple users. A workstation deployed as a single-user system is not considered a server.

19.8. **User:** See Authorized User.



Metro

Information Security Manager Training

Kent Swagler - CCEP
Director, Corporate Compliance
Direct line (314) 923-3097
Cell (314) 575-8334
kswagler@metrostlouis.org



Metro

Information Security Manager Training Overview

- What is Information Security (IS)?
- Why have an IS program?
- What are Benefits of an IS program?
- What are the Elements of an IS Program?
- Why do we have Data Classifications?
- What does 'Access Control' mean?
- What does 'Acceptable Use' mean?
- As IS Managers, what are your responsibilities?
- What are your co-workers responsibilities?
- What are some personal tips for your co-workers?



Metro

What is Information Security?

- Definition: *Protecting organization's information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Other familiar terms are:*

Computer Security

Information Assurance

- To be effective, Information Security must be on-going and daily process
- Part of organization's fabric



Metro

Why have an Information Security Program?

- Metro relies heavily on Information Technology (IT), and data in both electronic and paper form to perform it's mission
- Metro's IT network infrastructure and business applications must be protected from:
 - Potential sources of harm (physical and electronic)
 - Potential significant system / service failures or interruptions
- Agency and personal data must be protected from identify theft and misuse
- Information Security management works hand-in-hand with Records Retention management



Metro

What are the Benefits of Information Security?

- Prevent loss of Metro's information assets from damage
- Ensure electronic data security, confidentiality, integrity
- Access is known and monitored
- Prevent unauthorized access to Metro's IT network infrastructure and business applications
- Ensure the IT infrastructure and business systems are reliable and available for use



Metro

Essential Elements of an IS Program?

- Supported by Metro Senior Management
- IS management team consisting of:
 - IS Administrator (Compliance and Ethics Director)
 - Division IS Managers
 - Metro Vice President & Chief Information Officer (CIO)
 - IT Information Security Manager, IT technical staff
 - Computer Emergency Response Team (CERT)
 - All Metro employees
- Policy, standards, and procedures written and kept current
- IS Manager and employee education and training
- Periodic audits/reviews



Metro

Why do we have Data Classifications?

- Classified according to its use, sensitivity, and importance
- Metro's 3 Data Classifications:
 - **High Risk:** Disclosure would cause severe damage to Metro; legal, Federal, or State requirements for preventing disclosure
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Family Educational Rights and Privacy Act (FERPA)
 - ProCard numbers
 - **Confidential:** Disclosure would not expose Metro to loss, but should be protected (EADS performance reviews, employee address, phone number, family member names)
 - **Public:** Information that may be freely disseminated



Metro

What does 'Access Control' mean?

- Data access is limited to only those who need it for authorized purposes
- Users must not share usernames and passwords
- Terminated employees must have their accounts disabled
- System / Administrative accounts are closely controlled and monitored
- External access to Metro systems are limited, closely controlled and monitored



Metro

What does 'Acceptable Use' mean?

- Computer use must not interfere with Metro functions or employee's duties
- Use of Metro computer resources for personal profit is not permitted
- All software must be licensed to run on any Metro computer



Metro

What are Your Responsibilities as IS Managers?

- Work with Corporate Compliance Director to:
 - Educate employees on IS policy and procedures
 - Ensure employees are held accountable for following IS policy
 - Complete mandatory annual policy review and signature
 - Ensure employees use IT assets for business use only
 - Ensure all supporting contractors authorized to access Metro IT assets comply with IS policy
 - Serve as division/department contact for IS issues and incidents
 - Provide periodic feedback on division / department adherence to IS policy and standards
 - Can be provided as part of scheduled audits / reviews



Metro

What are Metro Employee's IS Responsibilities?

- Protect electronic and hardcopy data
 - Do not take sensitive / confidential data outside of Metro
 - Closely protect laptops and removable media (DVDs, flash drives)
- Do not write down or share user IDs and passwords
- Lock workstation screens
- Use at least 8-character alphanumeric passwords
- Log off and shut down workstation everyday
- Do not connect any device that was not procured through and installed by IT
- Do not use for personal profit or gain



Metro

What are Metro Employee's IS Responsibilities?

- Safeguard data and computer equipment from unauthorized access
- Do not disable virus protection or other security software
- Scan all removable media for viruses
- Use caution when deciding to open email attachments
- When you suspect a virus infection:
 - Stop using the workstation and leave it in its current state
 - Do not power the workstation off
 - Notify the IT Help Desk
 - Do not attempt to remove the virus



Metro

What are some IS Tips for your Co-Workers?

- Use anti-virus, anti-spyware, and anti-malware protection programs and keep them up to date
- Install and enable a firewall on your computer
- When shopping online, look for http**S**:// in the web address
- During an on-line purchase, look for the "lock" icon on the browser's status bar
- Watch what you post on Facebook, Twitter, etc.
- Inspect ATMs machine traps and swipe strips
 - Better yet, withdraw cash in a store or at your bank or credit union
- Only use credit cards for store and gas purchases



Metro

Any Other Questions and Comments?

My contact information:

Kent W. Swagler

Direct line (314) 923-3097

Cell (314) 575-8334

Fax (314) 335-3424

kswagler@metrostlouis.org

Ricoh Copier Scan to File Instructions

Overview

Your new Ricoh copier provides scanning functions to:

- Scan documents up to 11" by 17"
- Convert them to Adobe Acrobat PDF file or TIFF file format and then either:
 - Email them to yourself or another user using the **Scan to Email** function (**use this function for no more than five 8.5" by 11" pages**)
 - Save them on the copier's hard disk using the **Scan to URL** function for later retrieval (**use this function for all other scanning jobs due to the resulting file size and Agency email attachment 10 MB size limitations**)

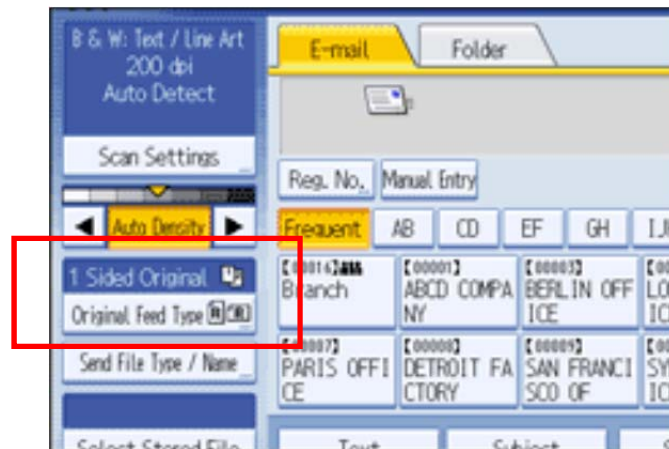
This guide provides the instructions for:

- Scanning to the copier hard disk and sending a Web URL link for your file
- Retrieving your scanned documents

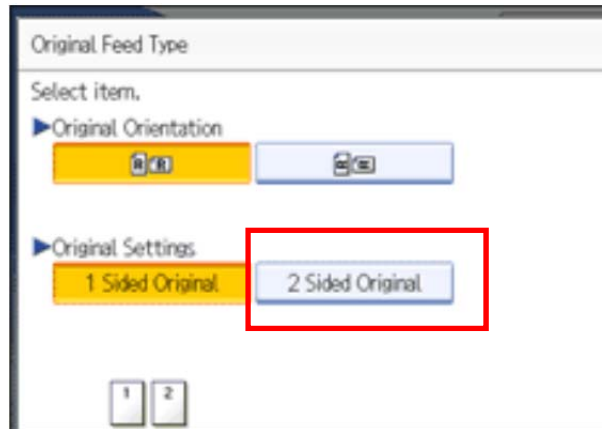
Important: To prevent the copier's hard disk from being filled with scanned documents, the copier is configured to store scanned files up to 30 days. Therefore, IT recommends users retrieve their scanned files from the copier as soon as they are scanned and stored.

Ricoh Copier Scan-to-Email Instructions

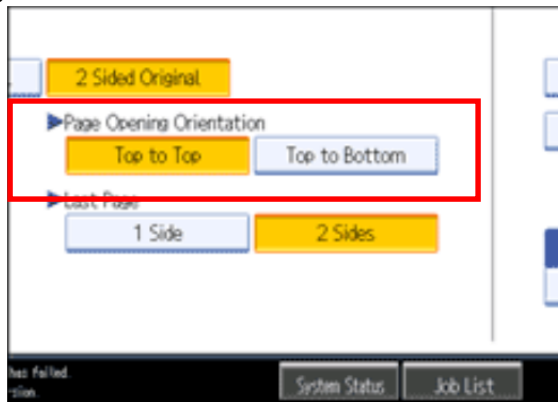
1. Press the **Scanner** button on your copier.
2. Place your originals in the document feeder.
3. Make sure the **E-mail** tab is highlighted.
4. **If your original is two-sided, follow the steps below. If your original has pages with color and you want to scan in color go to Step 5. Otherwise, go to Step 6.**
 - a. Press the **Original Feed Type** touch-screen button.



- b. In **Original Settings**, select **2 Sided Original**.



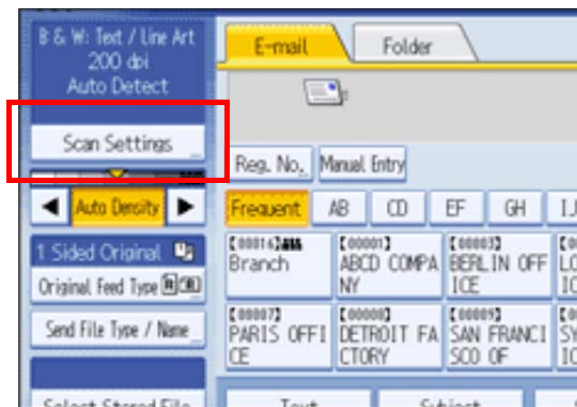
- c. In **Page Opening Orientation**, select **Top to Top** or **Top to Bottom** according to the binding orientation of the originals.



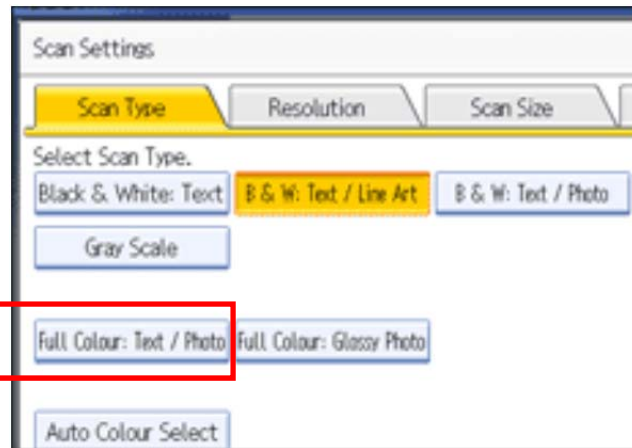
- d. Press the **OK** touch-screen button.

5. **Color originals:** If the original contains color pages and you want it to scan in color, you will need to use either a Ricoh MP 5001SP copier or a Savin 9050 copier. To scan in color:

- a. Press the **Scan Settings** button on the touch screen

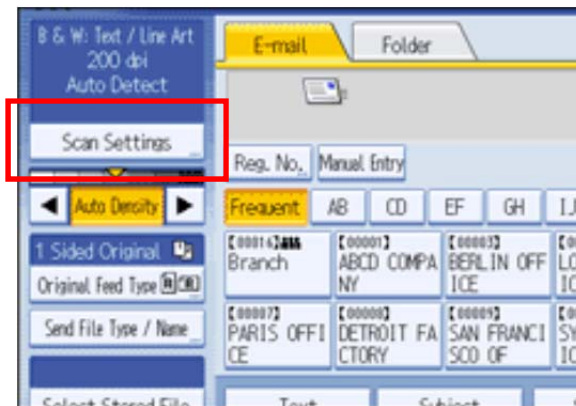


- b. Press the **Full Colour: Text/Photo** button on the Scan Settings touch screen. Press the **OK** button to return to the main touch screen.

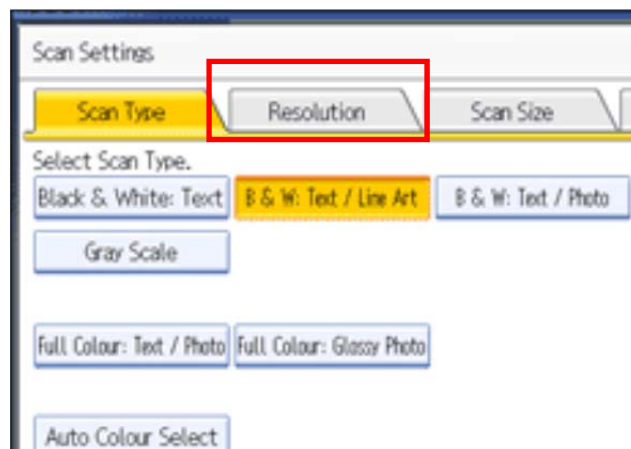


- c. Press the **OK** touch-screen button.

6. **Change Scan Resolution:** Press the **Scan Settings** button on the touch screen



- a. Press on the **Resolution** touch-screen tab



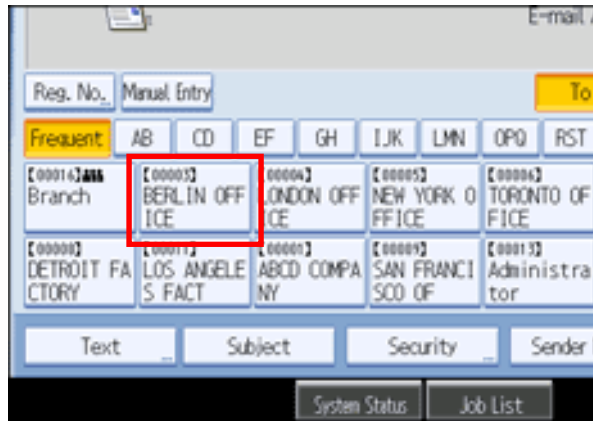
- b. Select [100 dpi], [200 dpi], [300 dpi], [400 dpi], or [600 dpi] as the scanning resolution.
- c. Press the **OK** touch-screen button.

7. **Select Scan Receivers:** Select the receiver(s) of your scan either by:

- Selecting them from the copier's address book; or
- Entering the e-mail address manually

a. Selecting the receivers from copier address book:

- i. In the address book, press the touch-screen button for the desired receiver name.

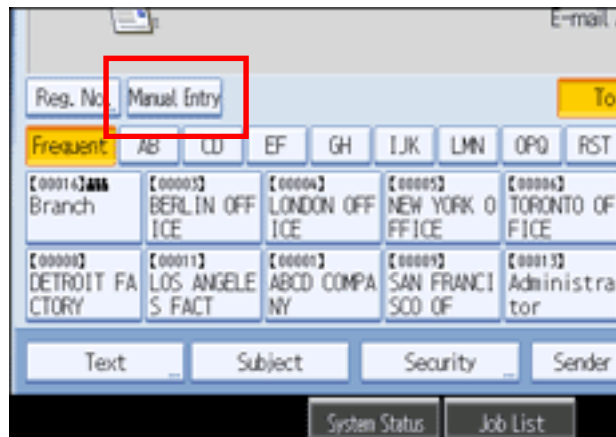


Result: The key of the selected destination is highlighted in gold, and the destination appears in the destination field at the top of the screen.

- ii. If the receiver name does not appear, press the [▲] or [▼] buttons

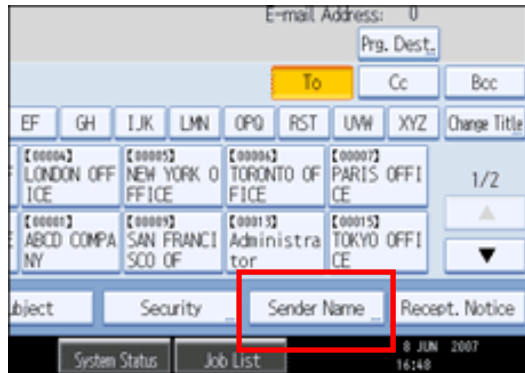
b. Entering the e-mail address manually:

- i. Press the **Manual Entry** touch-screen button

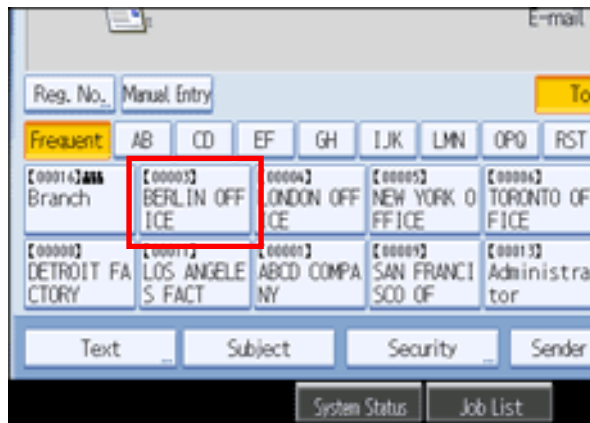


- ii. Enter the receiver's email address using the touch screen keyboard
iii. When done, press the **OK** button

8. **Select the Scan Sender:** You must select a sender for every scan-to email. To select yourself and/or someone else:
 - a. Press the **Sender Name** touch-screen button



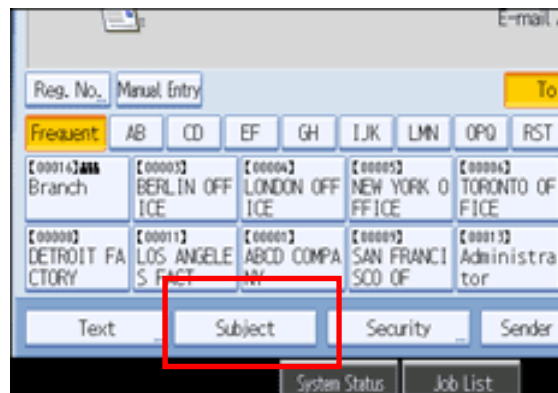
- i. In the address book, press the touch-screen button for the desired sender name(s) including yourself.



Result: The key of the selected destination is highlighted in gold, and the destination appears in the destination field at the top of the screen.

- ii. If the sender name does not appear, press the [▲] or [▼] buttons
 - iii. When done, press the **OK** button

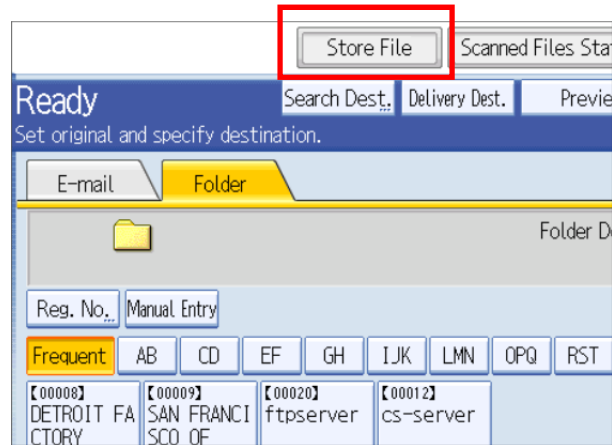
9. **Entering the E-mail Subject Line:** You can specify the subject for an e-mail when sending a file by e-mail.
 - a. Press the **Subject** touch-screen button.



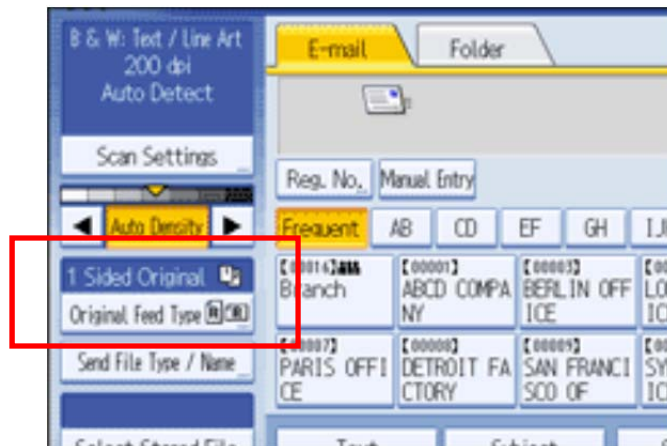
- b. Press the **Text Entry** touch-screen button; enter the subject line using the touch-screen keyboard.
 - c. When done, press the **OK** touch-screen button
- 10. When you have completed setting up your original and selected your receivers and senders, press the **Start** button to begin the scan.
- 11. Check your e-mail inbox to see if you received your scan. If you did not receive it, contact one of your receivers to see if he/she received it. If they did not receive it, contact your department Records Manager to assist.

Ricoh Copier Send and Store Scan-to-File Instructions

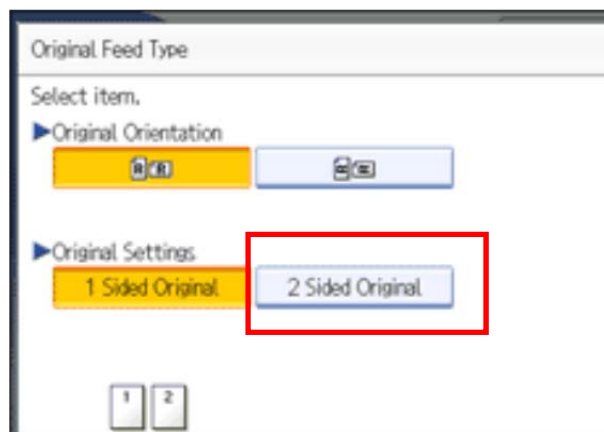
1. Press the **Scanner** button on your copier.
2. Press the **Store File** button on the touch screen.



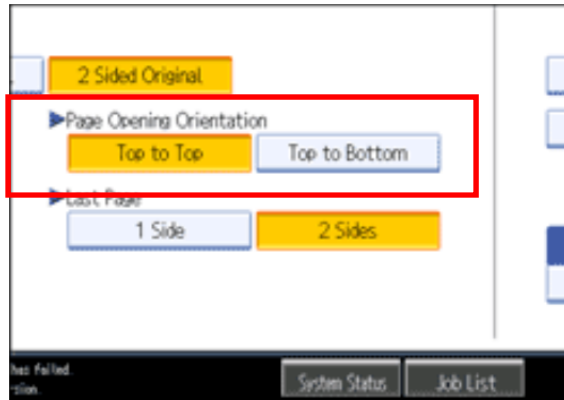
3. Press the **Send & Store** button. This will store your scanned document on the copier and send you a web URL link to your email account. Click the **OK** button.
4. **If your original is two-sided,**
 - a. Press [**Original Feed Type**] screen button on the touch screen.



- b. In **Original Settings**, select **2 Sided Original**.

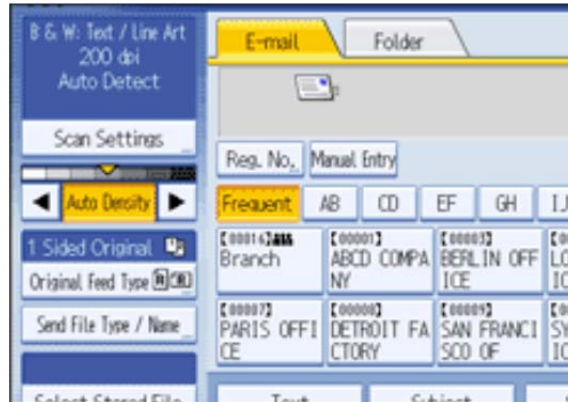


- c. 3. In **Page Opening Orientation**, select **Top to Top** or **Top to Bottom** according to the binding orientation of the originals.

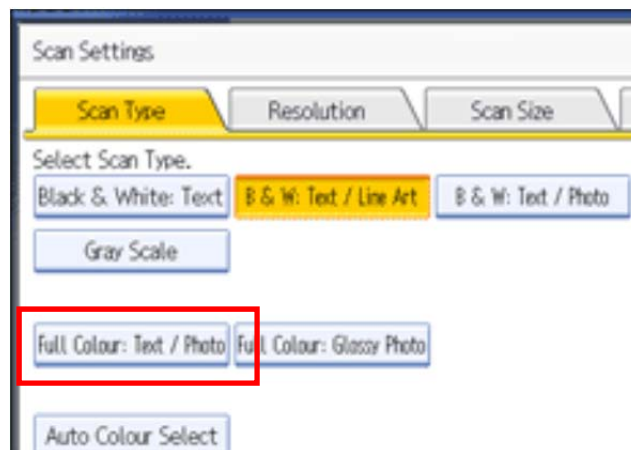


- 5. If the original contains color pages and you want it to scan in color, you will need to use either a Ricoh MP 5001SP copier or a Savin 9050 copier. To scan in color:

- a. Press the **Scan Settings** button on the touch screen



- b. Press the **Full Colour: Text/Photo** button on the Scan Settings touch screen. Press the **OK** button to return to the main touch screen.



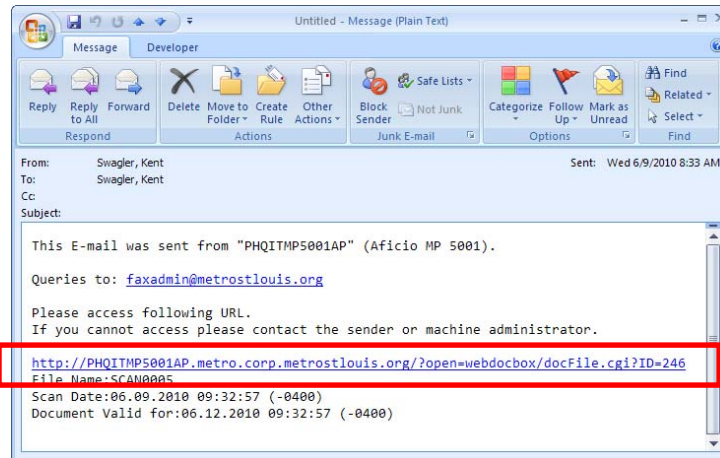
- 6. Select your **Receiver (To:)** email addressee by pressing the on-screen button containing the desired name or enter a different address manually by pressing the **Manual entry** button.

7. Select your **Sender (From:)** addressee by pressing the **Sender** on-screen button, the press the on-screen button containing the desired name, or enter a different address manually by pressing the **Manual entry** button.
8. Load your document into the scanner tray and press the **Start** button.

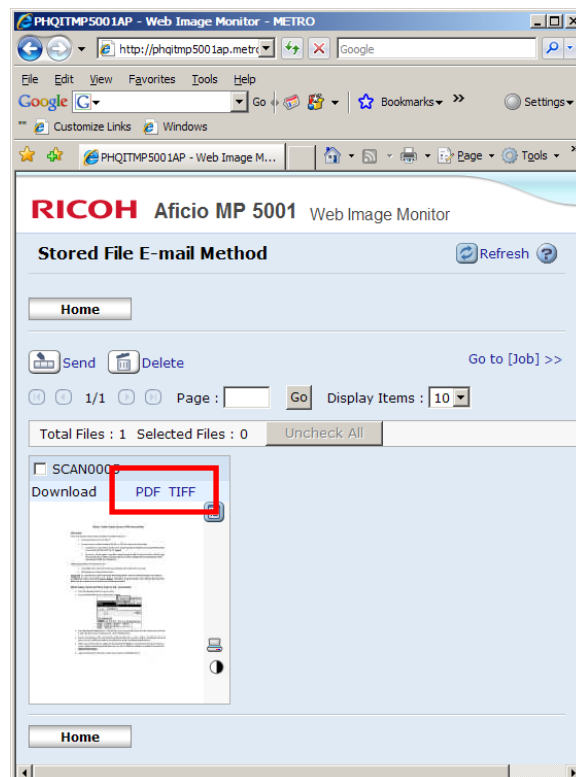
Scan-to-File Retrieval Instructions

To retrieve a file:

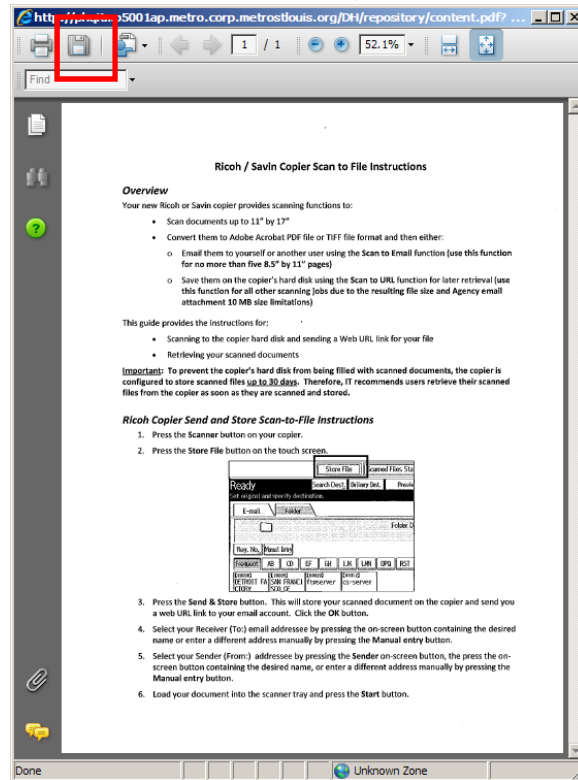
1. In the e-mail message you receive, click the URL for your scanned document



1. The copier's Web Image Monitor starts and shows all the current documents scanned to the copier. Find your document and click the **PDF** link. An Adobe PDF image of your document is displayed. (If you need to store it in TIFF format, click the **TIFF** link.)



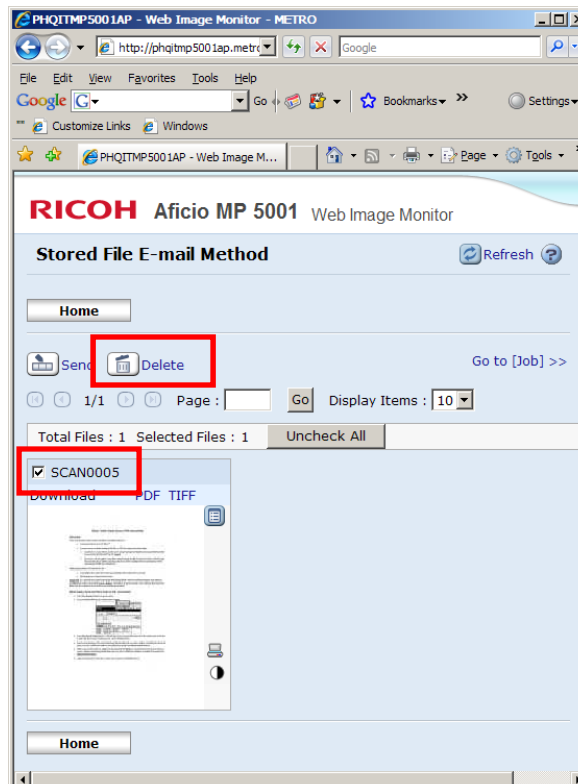
2. To save your document to a shared network folder, click the diskette icon.



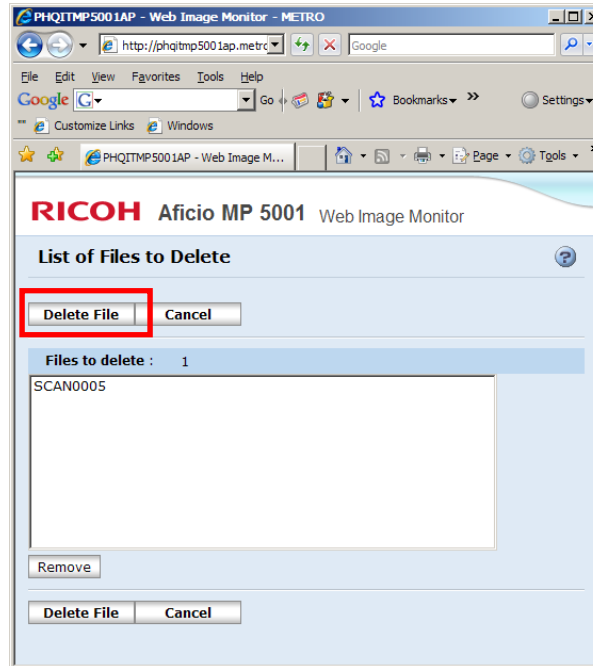
and select the desired storage location on a network drive folder.

3. Please delete the original file from the copier.

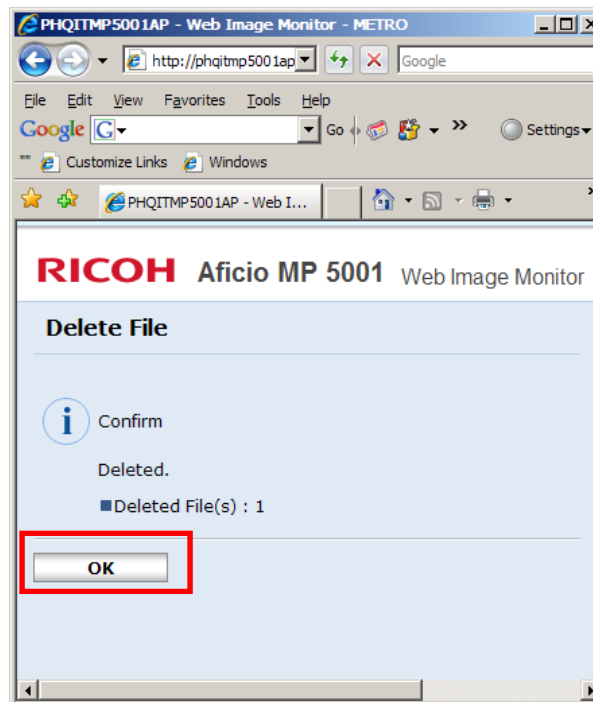
a. Fill in the checkbox by the scanned file name, then click the **Delete** icon



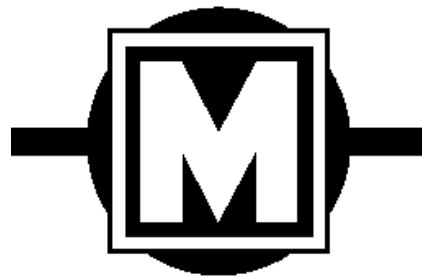
- b. Click the **Delete File** button.



- c. A confirmation screen is displayed. Click the **OK** button and close the screen.



**BI-STATE DEVELOPMENT
AGENCY D/B/A**



Metro

**RECORDS RETENTION
POLICY**

Table of Contents

1. BACKGROUND.....	3
2. PURPOSE AND OBJECTIVES	3
3. MANAGEMENT RESPONSIBILITY	4
3.1 Department Oversight	4
3.2 Legal Oversight	5
4. SCOPE/ APPLICABILITY.....	5
5. CATEGORIES OF RECORDS.....	6
5.1 Official Records:	6
5.2 Supporting Records:.....	6
5.3 Drafts:.....	6
5.4 Duplicate Records:	6
5.5 Personal Records:.....	6
5.6 Electronic Records:	7
5.7 Social Media Electronic Records:	7
6. CREATION OF RECORDS	7
7. LEGAL HOLDS.....	8
7.1 Implementation of Legal Hold:	8
7.2 Retention of Records Subject to a Legal Hold:.....	9
7.3 Termination of a Legal Hold:.....	9
7.4 Questions Regarding Legal Holds:	9
8. RETENTION AND DELETION OF EMAIL.....	9
8.1 Email Retained for Use in an Ongoing Matter:.....	10
8.2 Email Retained as a Business Record:	10
9. RETENTION AND DELETION OF SOCIAL MEDIA.....	10
10. CONFIDENTIALITY AND SECURITY	11
11. OFF-SITE RECORDS STORAGE.....	11
12. DISPOSAL OF RECORDS.....	11
ATTACHMENT 1 - RECORDS RETENTION SCHEDULE.....	12



Metro

RECORDS RETENTION POLICY

1. BACKGROUND

This Records Retention Policy addresses the storage, retention, and destruction of Bi-State Development Agency (BSDA) d/b/a Metro's electronic and paper business records. Attached to this Policy is a Records Retention Schedule that identifies the broad range of records and categories of records created by and/or retained by Metro, and that addresses the storage of such records (including the format and location).

The Agency's records may include virtually all of the documents produced by our employees, regardless of the form, including items that may typically be overlooked, such as inter-office email, desktop calendars, handwritten notes, etc. If there are questions about what is considered an Agency record, or what procedures to follow regarding records preservation, these should be directed to the Legal Department. Each Manager is responsible to ensure that the employees under his/her supervision understand the Policy and it is consistently and rigorously implemented, and each employee is responsible for fully cooperating. Failure to properly maintain the Agency's records could subject the Agency, as well as individual employees, to penalties and fines, charges of obstruction of justice and allegations of spoliation of evidence, and could seriously harm the Agency's position in litigation.

2. PURPOSE AND OBJECTIVES

The purpose of this Policy and the Records Retention Schedule is to facilitate the ease and speed of locating the Agency's records when needed for business purposes, when required by litigation, audits, requests by governmental entities, requests by local media, or for other reasons. Metro is committed to the effective management of records as business assets from the time they are created, through the required retention period, until they are destroyed. The objectives of this Policy are:

- To ensure that Metro's records are created, retained and destroyed in accordance with all applicable federal and state laws, ordinances and regulations;
- To provide guidance to Metro personnel regarding records management and the associated costs;
- To meet Metro's business needs by ensuring that records are available when needed, while minimizing the costs of retention and storage;

- To provide a reliable audit trail for important business transactions;
- To ensure that Metro is able to appropriately, systematically and securely dispose of records it is no longer required to retain;
- To ensure that records relevant to any on-going or anticipated litigation, audits, or governmental investigations are properly preserved in order to protect the interests of the Agency.

3. MANAGEMENT RESPONSIBILITY

Metro's Director of Corporate Compliance has been designated as the Records Administrator for the Agency. The Records Administrator has the primary responsibility for the day-to-day administration of the Records Management Policy. Metro staff who have questions about the Policy, need guidance regarding interpretation of the Policy, or who need to submit a request for storage or retrieval of particular records should email the Records Administrator at kswagler@metrostlouis.org. The Records Administrator is also responsible for overseeing the secure disposal of records once they are no longer needed.

3.1 Department Oversight

Each Department will designate a Records Manager within that department to assist the Records Administrator with implementing this Policy. These Records Managers are responsible for:

- Ensuring that the records of their respective departments are retained for the periods of time specified in the Records Retention Schedule;
- Assisting in the maintenance of an accurate and complete inventory of that Department's stored records;
- Coordinating with the Records Administrator to oversee the destruction of records in accordance with the Records Retention Schedule;
- Completing audits every two years in conjunction with the Records Administrator in order to ensure department records are in compliance with this policy.

3.2 Legal Oversight

To ensure that this Policy remains in compliance with all applicable statutes and regulations, General Counsel will serve as an advisor to the Records Administrator, and will be responsible for:

- Periodically reviewing and revising the Policy and Records Retention Schedule to ensure continued compliance with all applicable statutes and regulations;
- Evaluating future records management technologies as they pertain to the needs of the Agency;
- Ensuring that litigation holds are issued and enforced so that relevant documents are properly retained and the interests of the Agency are protected.

4. SCOPE/ APPLICABILITY

This Policy applies to all Agency electronic and paper business records created by Metro's employees, or that are in the custody or control of Metro's employees – no matter where they are located or in what form they are stored. All communications through Agency-related social media are considered public records and should be managed as such. All comments or posts made to Agency account walls or pages are public, not private.

Records are to be managed according to their content, not the form in which they were created or are being stored. The term "records" encompasses all written or recorded documents in whatever format or media they are retained - handwritten, typed, printed, photostatic or photographic, mechanically or electronically recorded, or other. Records may be in the form of, but are not limited to, paper documents, email, magnetic, optical or other electronic form, photographs, videotapes, and microforms. All records stored on all Metro information systems, related databases, shared network drives (k:\ and w:\), and personal network drives (u:\) are backed up on a daily incremental basis and full backups are performed weekly.

Records stored on employee workstations, CDs, DVDs, or flash/thumb drives cannot be remotely backed up. Therefore, it is very important for employees to store all important records on shared network drives that are backed up on a regular basis.

A Legal Hold may be prompted by a current or anticipated litigation, an audit, a governmental investigation, or other legal matter. It is a notice issued to an Agency department and/or to individual employees advising of the requirement to retain relevant records until the Hold is released (*see* Section 7). A Legal Hold overrides the Records Retention Schedule. An employee who violates this Records Retention Policy, including failing to honor a Legal Hold, may be subject to disciplinary action, up to and including termination.

5. CATEGORIES OF RECORDS

Agency records are categorized as follows:

5.1 Official Records:

These are records created or received and maintained as evidence of the Agency's business transactions and/or legal obligations. An official record includes the primary documents related to the transaction or legal obligation, plus all supporting records. Unless otherwise stated in the Records Retention Schedule, the Agency department that engaged in the transaction or legal obligation is responsible for preserving and maintaining the official record of that transaction or obligation, and for ensuring its disposal at the time required by the Schedule.

5.2 Supporting Records:

These are any documents or materials (e.g., email messages) that add critical or important information to an official record. Without them, the purpose or meaning of the official record would be incomplete or more difficult to understand. Supporting records are to be stored with the official record and are subject to the same retention period.

5.3 Drafts:

Only the final, executed version of records that are official records should be retained. Drafts should be promptly destroyed at the conclusion of a phase or a project unless the official records are subject to a Legal Hold. In that case, drafts should be retained along with the official record until the Legal Hold is terminated.

5.4 Duplicate Records:

As a general rule, as long as the original official record is retained, copies made for general business purposes should be disposed of as soon as they are no longer needed. Duplicates of original records that have been lost are to be retained and treated as original records.

5.5 Personal Records:

Private or personal records related to the Agency's business conduct are the Agency's property and not the individual employee. If an employee leaves the Agency, such records may not be removed from the Agency. They are subject to the Records Retention Policy and the Records Retention Schedule.

5.6 Electronic Records:

It is the Agency's policy that records should be retained only in electronic format whenever possible. Such electronic records **MUST**, however, be exact duplicates of the paper originals and be stored in a format that cannot be altered, such as a .PDF or other type of image file. Once those exact duplicates are stored on a network drive location or as an attachment in a Metro enterprise software application, then the paper original can be destroyed. Where a document, such as a letter, has been printed out and signed, it is not sufficient to save the unsigned word-processing version in lieu of the paper document. The signed copy must be scanned and saved. Electronic records must follow the same Record Retention Schedule as listed in Attachment 1. If there are discrepancies between electronic and hardcopy retention schedules, please contact the Agency Records Administrator.

5.7 Social Media Electronic Records:

Social media refers to the use of web-based and mobile technologies to turn communication into interactive dialogue. A social media website allows its users to interact with the site's creator and with each other as contributors to the site's content. Social media tools include blogs, microblogs (Twitter), wikis, video sites (YouTube), photo libraries (Flickr), networking sites (MySpace, Facebook), virtual worlds (Second Life), and other interactive sites.

6. CREATION OF RECORDS

Employees should be mindful of the following when creating records:

- Avoid creating too many records. Think about what you are creating, why, and with whom they are to be shared. Is it necessary to retain a document as part of the official record or as a supporting record? Is it a draft or final version? Can it be retained electronically? If it cannot be retained electronically, be prepared to justify why not.
- Telephone conversations are a good way to communicate, but think whether the information shared or agreed upon by phone should be confirmed in writing – by email, memorandum, or letter. If, for example, you received or imparted some critical information by voice mail, is it advisable to preserve that information in some fashion for later use?
- Limit the number of copies to only those who really need the information. Technology makes it easy and tempting to copy everyone who might conceivably have an interest in a matter. Employees are encouraged to distinguish between those individuals who need to be kept informed throughout the process or transaction, and those who only need to be aware of the end result.

- In order to facilitate retention in the correct records category, use clear captions on your records that correspond to categories in the Records Retention Schedule. This makes tracking, recovery, and disposition of records, particularly electronic records, much easier and faster.
- Social media sites may contain communications sent to or received by Agency employees, and such communications are, therefore, public records and must be kept available during the applicable retention period, per the current Agency Records Retention Schedule. These retention requirements apply regardless of the form of the record (digital text, photos, audio, or video, for example).
- Retain and manage copies of the files that you upload to social media sites such as YouTube and Flickr, which serve only as delivery points for moving images and photographs. Similarly, manage the content of Metro public or internal websites as you would your other records.

7. LEGAL HOLDS

Metro's policy is to retain and preserve all records that may be relevant to any government or civil audit, investigation, inquiry, or court proceeding, including lawsuits and arbitrations. The obligation to hold documents may arise before the Agency receives actual notice of a lawsuit, investigation, or other action. If such an action is even anticipated, employees are obligated to hold and preserve relevant records, and to consult with the Legal Department for further instructions. Any employee who alters or destroys Agency records, or takes any steps to impede a lawsuit, investigation, audit, or inquiry will be subject to discipline up to and including termination.

7.1 Implementation of Legal Hold:

When the Agency becomes aware of the need to preserve records due to a lawsuit, audit, investigation, or other inquiry, the Legal Department will send out a Legal Hold to the Records Manager of the affected department/s advising and to the Information Technology (IT) Division of the need to retain all relevant records. A Legal Hold notice suspends all requirements of the Records Retention Schedule that might otherwise apply to the records on hold. Once a Legal Hold is in effect, none of the affected records, including drafts and duplicates, may be altered or destroyed until the department receives written notification from the Legal Department.

If an employee becomes aware of the likelihood of an audit, inquiry, investigation or lawsuit, the Agency has not been formally notified or served and no Legal Hold has been

issued for the relevant documents, the employee must notify his/her manager, who should notify the Legal Department that a Legal Hold must be issued

7.2 Retention of Records Subject to a Legal Hold:

Records subject to a Legal Hold must be retained for the period during which the Legal Hold is implemented, or for the period specified in the Records Retention Schedule, whichever is longer.

For example, if a record that was created on February 1, 2005 and has a retention period of 5 years, was subject to a Legal Hold that was implemented in 2006 and terminated in 2008, that record should be disposed of on February 1, 2010. However, if a Legal Hold would still be in effect on February 1, 2010, the record should be retained until the Legal Hold is terminated.

7.3 Termination of a Legal Hold:

When a Legal Hold is terminated, the Legal Department will provide a separate written notice lifting the Hold. If no other Legal Holds are in effect relating to the pertinent records, they may be returned to their normal periods according to the Records Retention Schedule.

7.4 Questions Regarding Legal Holds:

Any Metro employee who has a question, issue, or concern about a particular transaction or event should notify his/her manager and the Legal Department, and should retain all relevant records relating to that transaction or event until the question/issue/concern is resolved.

All questions about the implementation and compliance with a Legal Hold should be directed to the Legal Department.

8. RETENTION AND DELETION OF EMAIL

Metro's email system is intended to be used for communication purposes and should not be used as an official records filing system. Metro restricts the size of employees' email boxes, and employees are discouraged from routinely saving all email. As a general rule, email communications that are not subject to a Legal Hold, and that are not required to be kept as part of an official record under this Policy and the Records Retention Schedule, should be deleted. All employees are required to review their email regularly and to delete email that does not meet one of these requirements.

In the event of a threatened or pending lawsuit, audit, investigation, or government inquiry, the same Legal Hold rules apply to email that apply to paper records.

8.1 Email Retained for Use in an Ongoing Matter:

Email that is retained for use in an ongoing matter, but is not part of the official or supporting records of a transaction or event, should be retained electronically in a controlled-access mailbox or public-shared electronic folder. When the matter to which it is related is concluded, email retained for use should be deleted unless it was shared with a third party and is important for the interpretation of final records, as described in Section 5.2 above.

8.2 Email Retained as a Business Record:

Email messages retained as official records or supporting records should be filed as separate records and retained by the employee/s maintaining them in compliance with the Records Retention Schedule. As much as possible, they should be kept electronically, secure from deletion, during their retention period.

9. RETENTION AND DELETION OF SOCIAL MEDIA

Because the technology is new, it is not yet clear to what extent traditional recorded retention and disposition practices apply to social media content on Metro public or internal websites or blogs, such as *NextStop*. Some basic guidelines for managing retention are:

- Determine whether content is substantial enough to constitute a record.
- Examine the content of the record and determine whether it would be covered by an existing retention schedule. For example, a web posting may be part of a project file, and other content may be equivalent to a Metro publication or press release.
- Manage emails and other communications sent or received via social media sites according to existing email retention and management procedures. You should equate email with correspondence for scheduling purposes
- Create content that will not pose a risk to the Agency if maintained on the Web indefinitely because destroying it according to the Records Retention Schedule may be a challenge. Some social media services may not delete profile or other information when an account is terminated, and information may be captured and used in ways not originally intended or contemplated.
- If you have new items that need to be added to the Retention Schedule, or if you have questions on existing items on the Schedule, contact the Agency Records Administrator.

10. CONFIDENTIALITY AND SECURITY

All Metro records must be kept and used in a manner that preserves their integrity and ensures that confidential or sensitive information is not disclosed to any unauthorized person. Records containing confidential or sensitive information should be clearly marked as such both individually and in their containing folders in order to make certain that all Agency employees with access understand that the information is to be protected. If records containing confidential or sensitive information are to be stored off-site, they do not need to be placed in separate storage boxes and marked with any “Confidential” markings. Identify those records storage boxes containing such information to your Department Records Manager and the Agency Records Administrator. They will use internal management controls to track those boxes and will coordinate with you whenever retrieval request for those boxes has been issued.

As with all hardcopy records, converting confidential or sensitive records to electronic storage and storing them in a named folder or designated storage location is highly encouraged.

If records containing confidential or sensitive information should be the subject of a discovery request during legal proceedings, the Legal Department will be responsible for determining what must be produced and what should not be produced.

11. OFF-SITE RECORDS STORAGE

All records covered by this Policy are to be retained and stored for the time periods designated in the Records Retention Schedule (unless, as previously indicated, the Schedule is superseded by a Legal Hold). Whenever possible, records should be stored in electronic format to minimize costs and provide easier access to them. In situations where storage space is limited or frequent access to records is not required, the Records Administrator may arrange for off-site storage.

12. DISPOSAL OF RECORDS

All Agency employees must cooperate with the Records Manager in their respective departments to review and evaluate the records in their custody on an annual basis to determine (1) if they are records that must be preserved, (2) what the required retention period is in accordance with the Records Retention Schedule, and (3) what the best medium and storage method is. Records that no longer must be retained under the Schedule, and are not subject to an existing Legal Hold, should be destroyed. All Records Managers should, in turn, coordinate with the Records Administrator.

Destruction of records is to be supervised by the Records Administrator. Records should be destroyed in a manner that makes them unreadable and their future use impossible – e.g. shredding paper records and using secure deletion or degaussing software for electronic records.

ATTACHMENT 1 - RECORDS RETENTION SCHEDULE

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
BUSINESS ENTERPRISES			
AIRPORT	All Contracts	Until termination	10 years
	Accounts receivable Journal	1 year	Permanent
	Payroll – Contract Employees	1 year	Permanent
	Sales Journal	1 year	5 years
	Invoices	1 year	7 years after payment
ARCH / PARKING GARAGE	All Contracts	Until termination	10 years
	Bond Redemption	1 year	Permanent
	Breakdowns, Arch Trams	1 year	4 years
	Bid specifications	2 years	Permanent
	Fare increases	2 years	Permanent
	Inspection & servicing of trams	5 years	Life of equipment
	Requisitions	1 year	2 years
	Daily revenue reports	1 year	2 years
	Signed Credit Card Receipts	1 year	2 years
SALES & MARKETING	All contracts	Until termination	10 years
RIVERBOATS	All contracts	Until termination	10 years
ECONOMIC DEVELOPMENT & REAL ESTATE	Correspondence	3 years	3 years
	Grant Applications	3 years	3 years
	Grant-funded project documentation	3 years	Permanent
	Contract documents	Until contract closeout / termination	10 years from date of contract closeout / termination
	Property Acquisitions	3 years	Permanent
ENGINEERING & NEW SYSTEMS DEVELOPMENT	All contracts	During term of contract	Permanent
	Closed project files/design & construction	1 year after completion	Life of facility
	Shop drawings/As built drawings	Life of structure or system	Life of facility
	General engineering consultant files	1 yr. after completion	Life of facility
	Annual Report, Consulting Engineers	1 year	Permanent
	Structure inspections	4 years	Life of structure
ARTS IN TRANSIT	All grants, grant applications and associated documents	During life of grant	Permanent
	All invoices and paid bill copies	1 year	2 years
	All project designs and drawings	During project implementation	Permanent
	All contracts	During contract term	Permanent

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
FINANCE	Account Reconciliations	1 year	5 years
	Annual Budget	10 years	Permanent
	Bonds, Industrial Revenue	Permanent	Permanent
	Debt obligations (bonds, long-term leases)	Permanent	Permanent
	Bonded indebtedness transcripts	Permanent	Permanent
	Structured lease transcripts	Permanent	Permanent
	General Ledger	1 year	Permanent
	Annual Report, Comprehensive Annual Financial Report (CAFR), A133	10 years	Permanent
	Invoice/Billing Support	Permanent. Since Jan 2005 Invoices are located in Oracle Payables application, and hard copied information uploaded to EDA application	Permanent until no longer using Oracle SCORE application/system
	Federal Financial Reports (FFR) Financial Statement Reports (FSR)	5 years after grant has gone inactive	Permanent
	Grants Records	Active, 1 year after grant has gone inactive	Permanent
	Echo	5 years after grant has gone inactive	Permanent
	Fuel Hedging	5 years	10 years
	Accounts Receivable: Paid Bill documents	1 year	2 years
	Accounts Receivable Ledger	3 years	3 years
	Paid voucher report	1 year	3 years
	Accounts Payable Journal Entries	Since Jan 2005 AP journals are located in Oracle Payables & General Ledger applications,	Permanent until no longer using Oracle SCORE application/system
	1099 forms hardcopy	3 years	7 years
	1099 electronic file	3 years	7 years
	Property titles and Easements	Until sold or terminated	10 years
	Vehicle titles, current and/or disposed	Until sold	Permanent
	Vehicle Registrations	Until sold	Permanent
	AP Vendor History	Permanent (Oracle)	Permanent (Oracle)
	Bad debts & collections	1 year	7 years after write-off
	Checks, paid/cancelled	2 years	Permanent
	Cash receipt journal	1 year	6 years
	Trust indentures, sale of bonds	Permanent	Permanent
	Bank deposit records	2 years	5 years

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
FINANCE (CONT.)	Disbursements journals	Since 01/05 AP journals are located in Oracle Payables & General Ledger applications,	Permanent until no longer using Oracle SCORE application/system
	Bank statements and reconciliations	2 years	5 years
	Sold vehicle titles	Until sold +5 years	Permanent
	Sold vehicle registration	Until sold +5 years	Permanent
	Appraisals	1 year	25 years
	Property, Plant & Equipment Fixed Asset Records	1 year	Permanent
	Bills of sale	1 year	Permanent
	JE Support	1 year	7 years
PASSENGER REVENUE	General Office Files	1 year	2 years
	Till Clerk Files	1 year	N/A
	Weigh Coin—cash verification system	1 year	2 years
PAYROLL	Weekly & Salaried timecards/labor distribution reports	10 years	20 years
	Records of additions to or deductions from wages	10 years	20 years
	Payroll Tax filing reports including, but not limited to 941s Schedule B, forms filed on Magnetic media	10 years	20 years
	Withholding Exemption Certificates (W4)	4years	10 years after separation
	Weekly/ Biweekly Payroll Gross-to-Net (GTN) Registers	20 years	20 years
	General Ledger Account Summary	5 years	N/A
	Pension Deduction reports/Arrears Balances	20 years	20 years
	Garnishment/Child Support Orders	5 years	20 years
	Employee W2 forms	20 years	Permanent
	Exception Earnings documents and Support Letters	5 years	20 years
	Vacation and Sick Leave Reports/Accrual Balances	20 years	Permanent
	Note: Requests for information from Benefits and Internal Audit departments have been as far back as 1980. Retaining timecards and labor distribution records when funded from bonds, grants or capital project funds require that we keep them until after the life of the bond or grant.		
PROGRAM DEVELOPMENT & GRANTS	Capital projects, grants	All documents associated with current and previous fiscal years	Permanent for all other records

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
RISK MANAGEMENT	Claim Files – No Payment (WC and Casualty) XXX files	1 yr past statute of limitations	n/a
	Claims Files (Worker’s Comp)	10 years after close	n/a
	Claim Files – Casualty	6 years after date of liability (DOL)	n/a
	Claim Files – Casualty (minors)	6 years after 18 th birthday	n/a
	Safety Certification documents	Life of system	n/a
	Bus/Van/LRV Inspections	2 years	5 years
	Report of Injury (see Worker’s Compensation)		
	Safety/Emergency Management Training	5 years	2 years
	Safety/Emergency Management Training documents and records	5 years	2 years
	State Safety & Security (SSO) Rail – Internal Audits	3 years	2 years
	SSO Three Year Reviews	6 years	3 years
	Vehicle safety improvement records (preventability)	3 years	3 years
	1099s	5 years	n/a
	Insurance policies and associated records	5 years	15 years after expiration
	Metro-issued Insurance certificates	3 years	5 years
	Insurance certificates received by Metro	6 years	n/a
	Safety/Risk investigations (including digital pictures)	6 years	n/a
	Corrective action plans (SSO)	2 years after close	6 years
	Education and training records	Retain while individual is performing the function, plus 2 additional years.	n/a
	Records from previous employers of Metro employees concerning drug and alcohol testing results	3 years after receipt of records from previous employers	n/a
	Negative test results and alcohol tests results less than .02	1 year from test date (2 years for MetroLink)	n/a
	Records related to the alcohol and drug collection process, random selection process, documents relating to decision to administer reasonable suspicion testing, and relating to post-accident testing	2 years	n/a
	Drug education and training records	Maintain while individual is performing the function + 2 years after individual leaves function	n/a
	Records from previous employers concerning drug and alcohol testing results of employees	3 years from receiving records from previous employers	n/a

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
GENERAL COUNSEL	Board of Commissioner Minutes & Committee meetings	10 years	Permanent
	Board Resolutions	10 years	Permanent
	Board By-laws and Policies	10 years	Permanent
	Board Administrative Files	10 years	Permanent
	“Sunshine” Law Requests	2 year s from date request is filled	5 years
	Subpoenas	2 years	n/a
	Legal files	2 years from date matter is concluded	Permanent
CORPORATE COMPLIANCE	Agency Off-Site Records control documentation	Permanent – stored on w:\drive	n/a
	Records destruction history	Permanent – stored on w:\drive	n/a
HUMAN RESOURCES	Employment applications, non employees	2 years	3 years
	Employment contracts	Until termination	10 years
	Active employee files	Until separation	n/a
	Inactive employees files	3 years after separation	12 years after separation
	Monthly personnel report	1 year	4 years
	Bids	3 years	7 years
	Injury Allowance Authorization	1 year	3 years
	Sick Leave Pay Application	1 year	3 years
	Corrective Action Plans/Performance Improvement Plans (PIP)	Until separation	12 years after separation
	Time Check / Termination Notice	1 year	3 years
	Accident/Sickness benefit claims	5 years	Permanent
BENEFITS	Active Employees Benefit File	3 yrs. post separation for Non-Vested / Electronic kept permanently beginning 2011	Merged w/Personnel File and kept 12 yrs. post separation unless HR changes to permanent
	Beneficiary File	3 yrs. post death / Electronic records kept permanently starting 2011	12 yrs. post death
	Call Recording System calls	6 months; Recorded calls are stored on data storage servers managed by IT	2 1/2 years in tape storage; 3 years total
	FMLA Claim Files	3 yrs. post close of claim	N/A
	Health & Welfare Summary Plan Descriptions	Permanently	Permanently
	LTD Employee Files	Until Retirement – then moved to Active Retiree Status	Follows retiree benefit file

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
	Pension Plan Documents	Permanently	Permanently
	Pension Payment/Deduction Reports	3 yrs.	Permanently
	Retiree Benefit File	3 yrs. post death / Electronically kept permanently beginning 2011	12 yrs. post death
	Terminated Vested Employees File	Until Retirement – then moved to Active Retiree Status	Follow retiree benefit file
	Union Contracts	Permanently	Permanently
	Vendor Contracts	3 yrs. post expiration of contract	7 yrs.
	Vendor Invoices/Payment Records	3 yrs.	7 yrs.
LABOR RELATIONS	Grievance files	3 years	7 years
	Arbitrators' decisions	1 year	Permanent
	Union contracts	Until termination	10 years
INTERNAL AUDIT	Audit reports, Internal	2 years	4 years
	Internal working papers	2 years	4 years
	Internal Audit Programs	2 years	Permanent
	Annual Report, audit/financial statements	1 year	Permanent
EXTERNAL AUDIT RECORDS	Audit reports, FTA Triennial	3 years	6 years
	Audit reports, External	2 years	4 years
	Internal working papers	2 years	4 years
	External Audit Programs	2 years	Permanent
	Annual Report, audit/financial statements	1 year	Permanent
INFORMATION TECHNOLOGY	Time records		Permanent
	All application/database backups (daily incremental and full weekly)	8 days for previous week's full backup tapes	Off-site–6 mo. cycle
	IT Disaster Recovery Plan and all associated documentation	Backup paper kept at Alternate Data Center	Permanent–reviewed & updated annually
	IT Equipment Inventory		Permanent – Reviewed and updated annually
OPERATIONS			
Stored in M5	Motor Fuel & Oil Consumption Report	1 year	3 years
Kept in KRONOS	Maintenance Time Cards	1 year	3 years
Kept in HASTUS	Daily Operator Sign-Up Sheets	6 months	25 ½ years
	Equipment parts manual	Life of equipment	n/a

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
OPERATIONS (cont.)			
Stored in M5. Repair Responsibility in Revenue Dept.	Farebox repairs	1 year	Life of equipment
Stored in M5. Repair Responsibility in Revenue Dept.	Farebox warranty items	Until expired	n/a
	Operator Station Files	During employment	25 years after separation
Stored in M5	Work orders, plant maintenance	2 years	3 years
Stored in SCORE	Requisitions	1 year	2 years
Stored in M5	Fire Inspection Reports	3 years	Permanent
	Shelter Cleaning Report	2 years	8 years
	Shelter repair log	2 years	8 years
Kept in HASTUS	Driving & on-duty time	1 year	6 years
	Daily Off-duty Report	2 years	2 years
VTrouble/Transit Master	Trouble dispatcher log	1 year	25 years
Stored on the W-Drive	Daily trouble sheet	1 year	25 years
Stored on the W-Drive	Supervisor daily log	1 year	6 years
	Accident investigation	1 year	25 years
Kept in HASTUS	ICC report	1 year	2 years
	Bus and LRV operator training files	1 year after separation	7 years after separation
	Bus operator follow-up ride slip	1 year after separation	7 years after separation
	Vehicle Safety Improvement Program	1 year	3 years
	Daily operator sign-up sheets	6 months	3 years
ADA SERVICES	Access Advisory Group Minutes	2 years	3 years
	Newsletters	3 years	Permanent, but may be stored electronically
	Senior/Disabled Reduced Fare Applications	2 years	3 years
	ADA Paratransit Applications & Materials	Active files: 2-4 assessment cycles with a 12-year maximum Inactive files – 2 years Deceased – 6 months	2 years
	Travel Training Records	Retain while individual is performing the function, plus 2 additional years	n/a
CALL-A-RIDE	Accident/incident reports	1 year	10 years
	Call Recording System calls	6 months; Recorded calls are stored on data storage servers managed by IT	None
	Employee Station Files	Until separation	Permanent

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
CALL-A-RIDE (CONT.)	Transportation Management Association (TMA) manifests	2 years	7 years
	CAR Daily Driving Assignment Forms	1 years	6 years
	CAR manifests	3 months	2 years
	Cash tickets for fare verification	3 months	2 years
	TMA Vendor deposits	3 years	None
CUSTOMER SERVICE (HQ & ALL METROBUS GARAGES)	Call Recording System calls	6 months; Recorded calls are stored on data storage servers managed by IT	2 1/2 years in tape storage; 3 years total
MAINTENANCE	Bus maintenance records : Daily repairs, inspection & maintenance logs, work orders, preventative maintenance inspection recap reports; engine, brake, transmission repair & overhaul records	2 years	Permanent (electronic in M5)
Stored in SCORE	Inventory Stock status	Permanent (real time status)	Permanent
Stored in SCORE	Daily Inventory Issue Tickets	Until ticket is closed	Permanent
Stored in SCORE	Purchase order report	1 year	2 years
Stored in SCORE	Weekly distribution report	1 year	2 years
Stored in M5	Daily parts transactions	1 year	2 years
Stored on the W-Drive	Road call logs	6 months	6 1/2 years
Stored in M5	Bus status	6 months	6 1/2 years
Stored in M5	Fuel and Oil sheets	6 months	5 1/2 years
Stored on the W-Drive	Monthly Revenue Vehicle Assignment sheets	6 months	20 years
Stored on the W-Drive	Coaches Out of Order Report	6 months	6 1/2 years
Stored on the W-Drive	Bus manufacturing specifications	Life of equipment	n/a
Stored in M5	Bus mileage	3 years	Life of equipment
Stored in SCORE	Inventory receiving orders	Until PO is closed	Permanent
MAINTENANCE OF WAY (MOW)	Inspection Records	12 months K:\Maintenance of Way\Maintenance Plans\MOW Inspection Archives	Permanent K:\Maintenance of Way\Maintenance Plans\MOW Inspection Archives
METROBUS OPERATIONS	Call Recording System calls	6 months; Recorded calls are stored on data storage servers managed by IT	None
	Radio Call Tape Recording (transcribed via WordNet software)	6 months; Recorded calls are stored on DVDs and retaining within MetroBus Operations Control	12 months in DVD storage; 18 months total
METROLINK OPERATIONS	Call Recording System calls	6 months; Recorded calls are stored on data storage servers managed by IT	None

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
TRANSPORTATION PLANNING & SYSTEM DEVELOPMENT	Implemented Planning Programs & Services	5 years	W Drive/Planning and Scheduling: 5 years
	Planning programs & projects	5 years	W Drive/Planning and Scheduling: 5 years
	Customer complaints & commendations	2 years	Trapeze COM: 2 years
	Transit Fare Data	2 years	W Drive/Planning and Scheduling: 2 years
	Call Center Internal Reports	2 years W Drive: Customer Service	n/a
SECURITY	Complaints/summons	5 years	10 years
	Customer Fare Checks	1 year	5 years
	Dispatcher Daily Radio Logs	3 years	6 years
	Incident Reports	3 years	10 years
	Invoices	3 years	5 years
	Platform and vehicle video/audio recordings	30-day hold for all platform video. When a specific video or audio is pulled, hold until matter is closed	1 year after matter is closed
	Undercover Police Security Program (UPSP) time reports	1 year	7 years
	Vehicle Pre-Inspections (before street patrol)	1 year	3 years
	Visitor logs	3 years	10 years
PROCUREMENT	Contracts, procurement	Until closeout	10 years from closeout
	Bid packages, procurement	Part of PO or Contract Record	n/a
	Bills of sale	1 year	Permanent
	Bid specifications, Arch	Part of PO or Contract Record	n/a
	DBE Reports, Annual	5 years	Permanent
	DBE reports, Bidders' Responses	Part of PO/contract record	n/a
	DBE reports, monthly	1 year	10 years
	Purchase Orders, procurement	Oracle	n/a
	Quote Packages, procurement	Part of PO/contract record	n/a
	Requisitions	Oracle PO file	n/a
	Requisitions, Arch	Oracle PO file	n/a
	Requisitions, procurement	Oracle PO file	n/a
	Vendor history	Permanent	Permanent

<u>DEPARTMENT</u>	<u>TYPE OF RECORD</u>	<u>RETENTION IN DEPARTMENT</u>	<u>RETENTION IN STORAGE</u>
SALES & MARKETING			
METRO RIDE STORE, ARCH & RIVERBOAT SALES	Arch Sales Call Recording System calls	6 months; Recorded calls are stored on data storage servers managed by IT	2 1/2 years in tape storage; 3 years total
COMMUNICATIONS	Bi-State publications (newsletters, annual reports, brochures, etc.)	3 years	Permanent, but may be stored electronically
	Media releases and Social Media entries	3 years	Permanent, but may be stored electronically
WORKFORCE DIVERSITY/EEO	EEO Report, New Hires	1 year	9 years
	EEO Report, Promotions	1 year	9 years
	EEO Report, Suspensions	1 year	9 years
	EEO Report, Termination	1 year	9 years
	EEO Annual Report	1 year	Permanent
	EEO Reports, Discrimination Charges	1 year	Permanent
	EEO Report, Major Job Categories	1 year	Permanent
	EEO Report, Title VI & Civil Rights Investigations	1 year	9 years



Metro

Records Manager Training



Kent Swagler
Director, Corporate Compliance



Metro

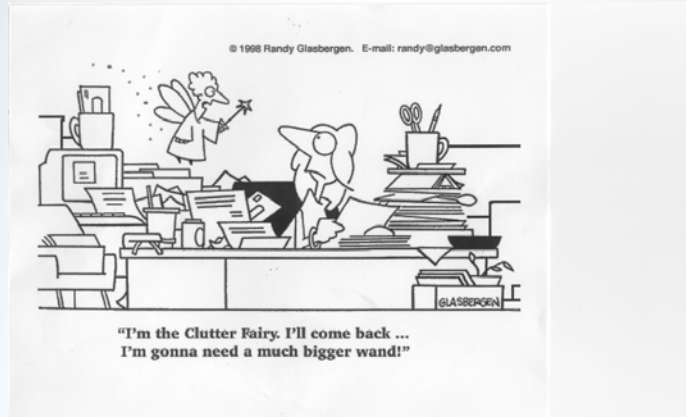
Agenda

- Compliance Impacts and Recent Events
- What are "Records"?
- Records Retention
- Records Holds
- Records Storage and Retrieval
- Records Disposal
- Related Issues
- Questions?



Metro

Sometimes, Records Management can seem like this.....



As of September 12, 2013

3

Metro Moves The Community Forward



Metro

Records and Information is Everyone's Responsibility

- **Records Matter**
 - That is why organizations spend money saving them
 - It is why we have policies to manage them
- All Employees are Responsible for Following those Policies
- Failing to do so Can Have Effects That May Be Felt for Years to Come

As of September 12, 2013

4

Metro Moves The Community Forward



Metro

Rising Stakes of Records Management - Regulatory Compliance

- The Legal Landscape has changed. In the last 7 years, there have been dramatic changes to regulations that impose requirements on management of corporate records.
 - Sarbanes Oxley (SOX)
 - Gramm Leach Bliley (GLB)
 - Healthcare Insurance Portability and Accountability Act (HIPAA)
 - Amended Federal Rules of Civil Procedure
 - and others

As of September 12, 2013

5

Metro Moves The Community Forward



Metro

Rising Stakes of Records Management - Financial Impact

- Storage and management expenses
- Lawsuits, judgments and settlements
- Sanctions (court, regulators)
- Harm to public image and value to community
- Personal liability for senior management

As of September 12, 2013

6

Metro Moves The Community Forward



Metro

Rising Stakes of Records Management - Financial Impact

- Records Storage: American Express Financial Advisors fined \$300,000 for failing to keep customer account statements in the required format
- Records Destruction: Court imposes \$1 million fine on Prudential for records destruction after the company fails to adopt an effective records management policy
- Email: American Home Products Corporation settles for nearly \$3.75 billion, as a result of an e-mail exchange depicting an irreverent attitude toward the potentially harmful effects of its weight-loss drugs



Metro

Agenda

- Compliance Impacts and Recent Events
- **What are “Records”?**
- Records Retention
- Records Holds
- Records Storage and Retrieval
- Records Disposal
- Related Issues
- Questions?



Metro

Our Records

- You may have communication, investigative, and/or analytical duties in your work
- Your communications, investigations, or analyses become **records** — regardless of their form
- Purposes of records:
 - **To document** what has occurred for future use
 - **To comply** with laws and regulations
 - **To share** an idea, to state a position or to **clear up confusion**



Metro

What Are "Records"?

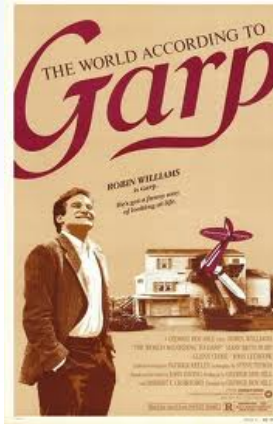
- Most things you write down, record, or produce as an employee
 - Handwritten notes
 - Contracts and forms
 - E-mail and voicemail messages
 - Letters, memos, and faxes
 - Computer data
 - Desk calendars
 - Appointment books
 - Expense reports





Metro

Generally Accepted Recordkeeping Principles (GARP)



As of September 12, 2013

11

Metro Moves The Community Forward



Metro

Generally Accepted Recordkeeping Principles (GARP)

Records must be created, organized, secured, maintained, and used in a way that effectively supports the activity of that organization, including:

- Facilitating and sustaining day-to-day operations
- Supporting predictive activities such as budgeting and planning
- Assisting in answering questions about past decisions and activities
- Demonstrating and documenting compliance with applicable laws, regulations, and standards



As of September 12, 2013

12

Metro Moves The Community Forward



Metro

Generally Accepted Recordkeeping Principles (GARP)

Accountability

- Senior executive assigned to oversee record retention program, delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure program audit-ability

Integrity

- Records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability

Protection

- Ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity

Compliance

- Comply with applicable laws and other binding authorities, as well as the organization's policies



Metro

Generally Accepted Recordkeeping Principles (GARP)

Availability

- Ensures timely, efficient, and accurate retrieval of needed information

Retention

- Maintain records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements

Disposition

- Provide secure and appropriate disposition for records that are no longer required to be retained by applicable laws and the organization's policies

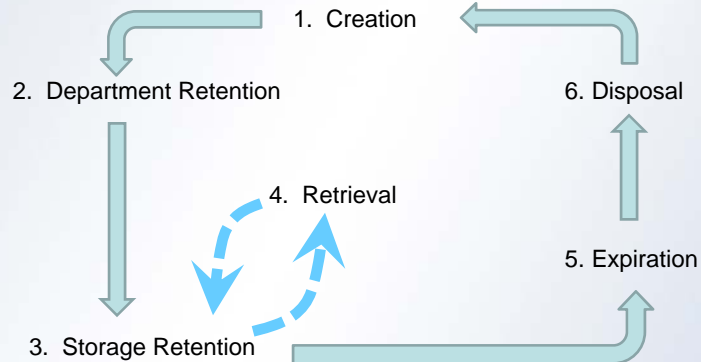
Transparency

- Record retention program's processes and activities are documented and available to all personnel and appropriate interested parties



Metro

Life Cycle of a Record



Metro

Pop Quiz!

- Which of the following would probably be considered a "record"?
 - A voicemail message
 - Handwriting on scratch paper
 - A calendar
 - A deleted e-mail
 - All of the above





Metro

Who Reads Our Records?

- Consider who might read your records — even **beyond intended recipient**:
 - Supervisor/co-workers
 - Government officials
 - Lawyers
 - Public



Metro

Who Reads Our Records?

- Our records could "go public" in the future —
 - By publication in newspaper or magazine
 - As result of government inspection/audit
 - In due-diligence process
 - In discovery phase of a lawsuit
- **Ensure that your records would reflect well if held up to close scrutiny**





Metro

Electronic Communication Guidelines

- What is considered Electronic Communications?
 - E-mail, instant-messaging, and other electronic tools
- Consider all your electronic communications as official records
- Forward electronic communications judiciously
- Confidential information should be encrypted
- Instruct recipients about confidentiality



As of September 12, 2013

19

Metro Moves The Community Forward



Metro

Creating Accurate Records

- Guidelines for creating complete and accurate records:
 - Before creating record of event, **get the whole story**
 - **Don't exaggerate** or use overly dramatic language
 - **Be objective**
 - **Be concise** and careful with wording
 - **Avoid creating records in haste** or when you feel emotional
 - See the records as **formal business documentation**
 - **Review contents** of e-mail and **double-check recipient list**
 - Once it is considered official or published, **delete all drafts**



As of September 12, 2013

20

Metro Moves The Community Forward



Metro

Agenda

- Compliance Impacts and Recent Events
- What are “Records”?
- **Records Retention**
- Records Holds
- Records Storage and Retrieval
- Records Disposal
- Related Issues
- Questions?



Metro

Records Retention - Legal Requirements

- **Required by law** to maintain certain records for specified periods of time
- Records Retention Policy provides guidelines on:
 - What records to keep and for how long
 - How to dispose of them
- If you have questions about the policy, **ask your Supervisor and Records Administrator (Kent)**





Metro

Purpose & Scope of Records Retention Policy



- Records Retention Policy Goals
 - Complying with relevant state/federal laws and regulations
 - Maintaining security/privacy of our records
 - Having systematic plan for records destruction
- Policy applies to:
 - All printed documents and electronically stored records
 - All employees, contractors, and anyone working on our behalf
 - All branches, divisions, and subsidiaries throughout Metro



Metro

Metro's Records Retention Policy





Metro

Records Retention Periods are determined by:

- **Legal and regulatory** – Federal, state, local, and even international laws
- **Fiscal** – Ensure the timely obligation payments, receipt of receivables, and support financial audits and tax returns
- **Operational** – Once previous requirements have been established, determine how long records are needed to satisfy Metro business needs
- **Historical** – Records that depict Metro history should be preserved for the life of Metro.
 - Examples: Articles of incorporation, bylaws, charters, news articles, and board of directors' minutes



Metro

Pop Quiz!

To save time, Fred, a company manager, keeps duplicates of important files at his home office, locked in a drawer for safekeeping. When the company began its annual review of documents for retention or disposal, Fred didn't include the files he had at home. Was this okay?

- a) Yes, because company managers can make exceptions to the Record Management Policy for their own files.
- b) Yes, because files kept off-site are not covered by the Record Management Policy.
- c) No, Fred needs to include all files in the record-retention review — even those kept at his home office.





Metro

Agenda

- Compliance Impacts and Recent Events
- What are “Records”?
- Records Retention
- **Records Holds**
- Records Storage and Retrieval
- Records Disposal
- Related Issues
- Questions?



Metro

Suspension of Record Destruction – Legal Holds

- We have legal obligation to preserve documents related to legal proceeding or government investigation
- Report potential litigation, investigation, or audit to Legal Department immediately
- Legal Department may issue Legal Hold Order specifying records to be preserved until further notice
- Employees should not alter/dispose of records under hold order — even if scheduled for destruction
- Email and hardcopy notification by Legal Counsel



Metro

Agenda

- Compliance Impacts and Recent Events
- What are “Records”?
- Records Retention
- Records Holds
- **Records Storage and Retrieval**
- Records Disposal
- Related Issues
- Questions?



Metro

Hardcopy Records Storage Procedures

- Storage boxes through Staples ([Item # 825695](#))
- Boxes organized by assigned Control Number (2012xx)
 - Max 20 boxes / Control Number
- Send Control Number request to Records Administrator (RA)
- RA emails numbers and content list template worksheet
- Organize your records to fit department needs (fiscal year, project, function, etc) and fill boxes



Metro

Hardcopy Records Storage Procedures

- Complete records list worksheet and email back to RA
- RA will schedule pickup
- Records securely stored at:
 - Illinois Bus Records Room (HQ and all Illinois facilities)
 - Brentwood Records Room (all MO facilities west of HQ)



Metro

Hardcopy Records Retrieval Procedures

- Email Control Number and box numbers to RA
- RA will coordinate with Support Services for retrieval and delivery
- When done, email RA to have the boxes picked up
- RA will coordinate with Support Services for pickup and return to records room



Metro

Electronic Records Storage

- Organize your records to fit department needs (fiscal year, project, function, etc) and store in folders on network drives (w:\, k:\, u:\)
- **RECORDS MANAGERS** responsible for records management that includes:
 - Storage
 - Retention
 - Destruction
- Will be periodically audited by IT, RA, and Internal Audit



Metro

Agenda

- Compliance Impacts and Recent Events
- What are "Records"?
- Records Retention
- Records Holds
- Records Storage and Retrieval
- **Records Disposal**
- Related Issues
- Questions?



Metro

Records Disposal

- Documents scheduled for disposal must be destroyed in safe, secure, and environmentally sound manner
- Printed documents should be shredded
- All copies should be destroyed
- Electronic documents and back-up copies should be deleted
- Transfer files stored on workstation and laptop hard drives to a network drive folder then disposed when expired
- Electronic communications must be categorized by content/ audience for retention/destruction purposes



As of September 12, 2013

35

Metro Moves The Community Forward



Metro

Records Disposal

- Hardcopy:
 - Records destruction days scheduled every 6 months at all storage rooms
 - Monthly and/or as-scheduled shreds scheduled at facilities with confidential storage bins
- Electronic:
 - Recommend scheduling department reviews and destruction days every 6 months as well
 - RA will publish annual electronic records audit schedule
 - Goal: audit every department every two years
 - Internal Audit will include electronic records reviews as part of scheduled department / project audits

As of September 12, 2013

36

Metro Moves The Community Forward



Metro

Agenda

- Compliance Impacts and Recent Events
- What are “Records”?
- Records Retention
- Records Holds
- Records Storage and Retrieval
- Records Disposal
- **Related Issues**
- Questions?



Metro

Related Issues

Modification of Policy

- We may modify Policy or Schedule at any time
- Employee suggestions for modifications should be sent to Legal Department
- Decisions to re-classify records should be reviewed by Legal Department





Metro

Penalties for Violation

- Any employee who violates Policy will be subject to discipline, up to and including termination of employment
- Anyone who knowingly alters, destroys, conceals or falsifies records could be fined, imprisoned for up to 20 years, or both



As of September 12, 2013

39

Metro Moves The Community Forward



Metro

What are Your Roles & Responsibilities?

- All Metro employees recognize and understand the obligation they have to create, maintain, dispose of, and preserve records
- Records you create while a Metro employee generally **DO NOT** become your personal property
- Metro records may be on personal devices such as smart phones, blackberries, iPads, home computers, and in the cloud (Gmail, Facebook, etc.); Employees are responsible to follow Metro's policies regarding protection, security, and retention of this information

As of September 12, 2013

40

Metro Moves The Community Forward



Metro

What are Your Roles & Responsibilities?

- Official department records belong to Metro and must be managed in accordance with our Records Retention policy
- Some incidental personal records are expected and those should be maintained separately
- **All of us are Records Managers**



Metro

Rules of Records Management

- *If you don't need it, don't keep it.*
- *If you do need it, keep it in a way you can find it.*
- *The more you keep, the harder it is to find.*
- *If it is worth more, spend more to protect it.*



Metro

Any Other Questions and Comments?

- My contact information:

Kent W. Swagler

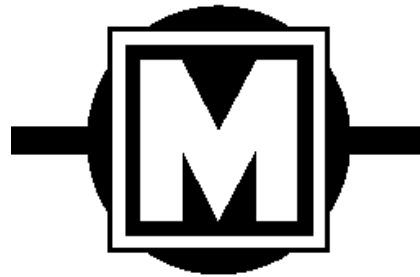
Direct line (314) 923-3097

Cell (314) 575-8334

Fax (314) 335-3424

kswagler@metrostlouis.org

**BI-STATE DEVELOPMENT
AGENCY D/B/A**



Metro

**ELECTRONIC RECORDS
MANAGEMENT PROCEDURES**

Contents

Overview	3
Electronic Storage Capabilities provided to Authorized Metro Employees	3
Department/Division Electronic File Plan	4
EMAIL RECORDS MANAGEMENT	7
Storing Business Emails.....	7
Deleting Emails.....	7
Emptying the Wastebasket.....	8
Recovering Emails Deleted from the Wastebasket	9
Archiving Email Folders.....	10
Accessing your Email Archive Folder through Email.....	14
Searching for Expired Emails – Active Inbox and Archive Email Folders	17
Searching for Expired Electronic Files in Network Drive Folders.....	21

Overview

Managing your email and other electronic records so you are in accordance with Metro's Records Retention Policy is like managing hardcopy records; you have to regularly review your documents and folders, purge them of all expired records, and have them destroyed. Although it does take time to complete these steps initially, the effort involved is much easier and the time commitment is much less, because it only requires mouse clicks and keystrokes on your workstation versus going through file cabinets, file folders, and storage boxes.

With some collective planning, organizing, and time commitment, your department's Records Manager and you can organize your electronic records to make the retention, review, and disposal process much easier and quicker to perform.

Additionally, whenever the General Counsel is required to issue a Legal Hold and your department's records are subject to an e-discovery request, or if you are out of the office for an extended period of time and your supervisor needs to find some work-related documents, finding those records will be much easier because of your on-going effort to comply with these procedures.

This document is designed to guide you through the process of:

- Organizing your department's/division's electronic records
- Organizing and retaining your individual and department business records on your k:\, w:\, and u:\ network shared storage drives
- Archiving key business-related email documents to help you not to exceed your e-mail account size limit
- Purging your email account and your email archive of expired email records
- Purging your individual and department business records on your k:\, w:\, and u:\ network shared storage drives

Electronic Storage Capabilities provided to Authorized Metro Employees

Depending on his/her job responsibilities, a new employee's supervisor can request the Information Technology (IT) division to set up one or more of the following before a new employee reports for the first day of work:

- An email account
- Access to one or more folders in the K:\ or W:\ shared network folder
- The employee's own private U:\ drive (User drive) for personal or confidential work-related documents

A new employee who receives any or all of these privileges is now considered a Records Manager for work files her/she creates and/or manages as defined in the Metro Records Retention Policy. As a result, he/she must manage electronic and hardcopy records in accordance with the Policy.

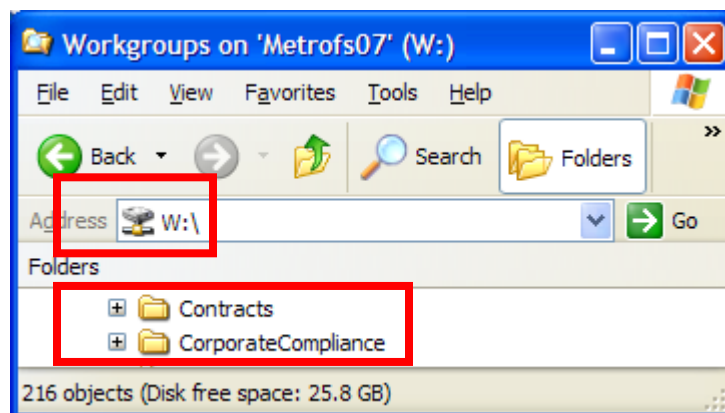
As part of their initial training at Metro, and annually thereafter, new employees must review the Records Retention Policy and successfully pass the on-line quiz. The Records Retention Policy and many other policies and procedures are kept on-line through Metro's Policy and Procedure Manager (PPM) system. As part of the new employee setup request, when a supervisor requests IT to provide a new employee with email access, they are automatically set up to access the PPM system .

Once given access, the employee can click the following link to access the Records Retention Policy: [Records Retention Policy](#). For any access issues or additional assistance, please contact the Director of Corporate Compliance, who is the Agency's Records Administrator.

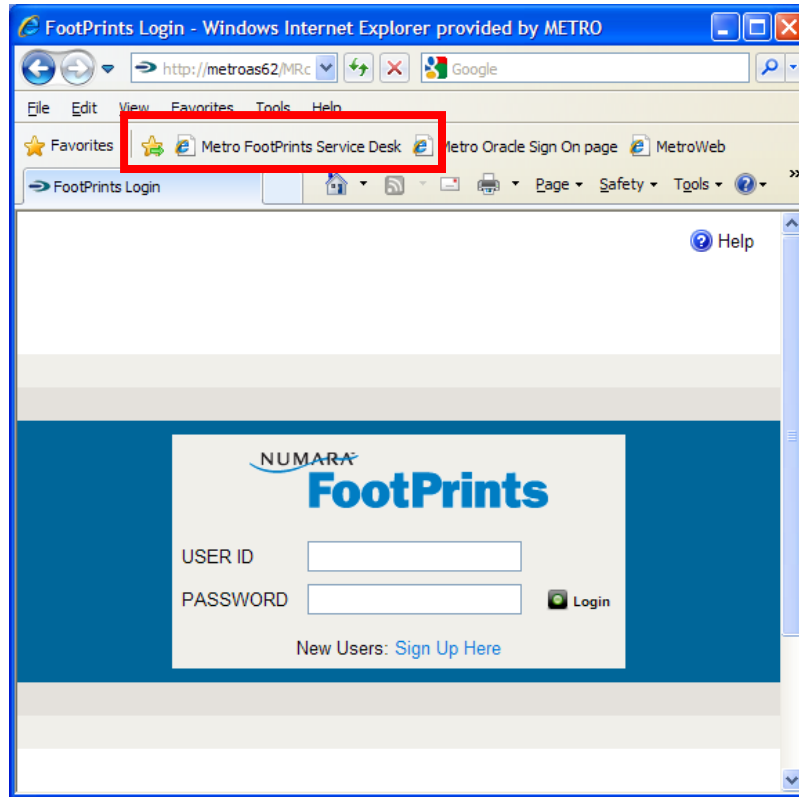
Department/Division Electronic File Plan

If an electronic records storage/ file plan for your department/division has not been defined, your Division/Department Records Manager(s) is responsible for leading an effort to define it, document it, and distribute it to everyone in your department/division before proceeding to organize your records, so that everyone retains their electronic records in accordance with the same file plan. Recommended parts of this plan should include:

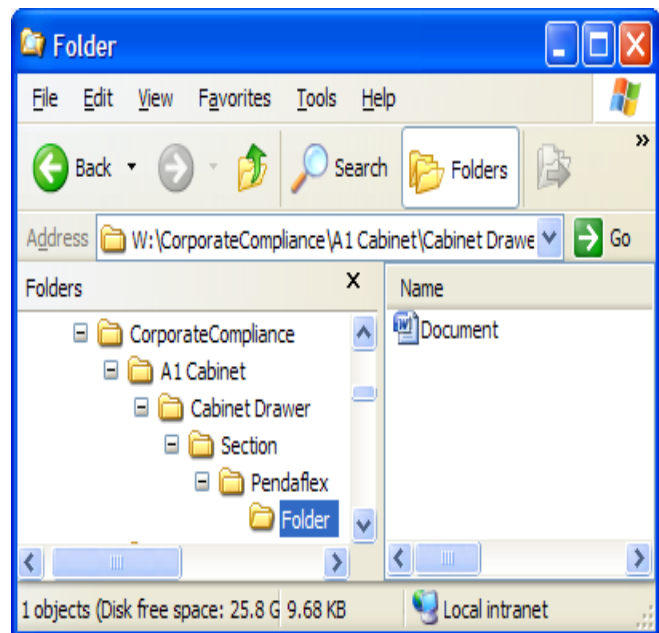
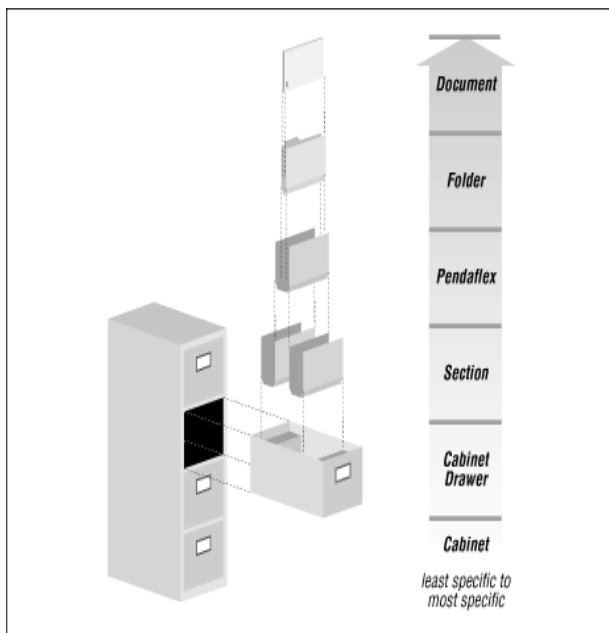
- A root department/division file folder on either the K:\ network drive (used by MetroLink Operations and Maintenance) or the W:\ network drive (e.g., W:\Human Resources, W:\CorporateCompliance)



Note: Only IT support staff can create new root files folders. To request a new root folder, submit an IT Request form through the Metro's web-based Footprints IT Service Desk application.



- A tree-structured, or hierarchical file folder directory, where each main file folder represents a department name, primary business function, project, facility, or other significant criteria. The directory can mirror a typical office file cabinet as shown in the example below:



- Documents stored in the file plan are organized, retained, and eventually deleted in compliance with the department and division's records retention schedule as listed in Attachment 1 of the [Records Retention Policy](#)
- Sub-Folders with folder names containing 30 characters or less as much as possible. To ease the records review process, an expiration date (e.g. "MM-YY") or a retention period (e.g. XX yrs) should be included as part of the folder name.

Once the department/division file plan has been completed, you must:

1. Create the file folders and sub-folders in accordance with your file plan
2. Reorganize your existing electronic records by:
 - a. Identifying and deleting all expired records
 - b. Identifying and deleting all personal non-business related records
 - c. Moving all remaining records into the file plan folders you have just created
3. Repeat steps 1 and 2 for your email records
4. Have your department/division Records Manager(s) schedule and conduct electronic records reviews to delete all expired records every six months.

Please note: If files are accidentally deleted, they can be recovered from previously completed system backups. Please contact the Help Desk at extension 5555 to submit a file recovery request.

Note, however that any files created and accidentally deleted the same day cannot be recovered.

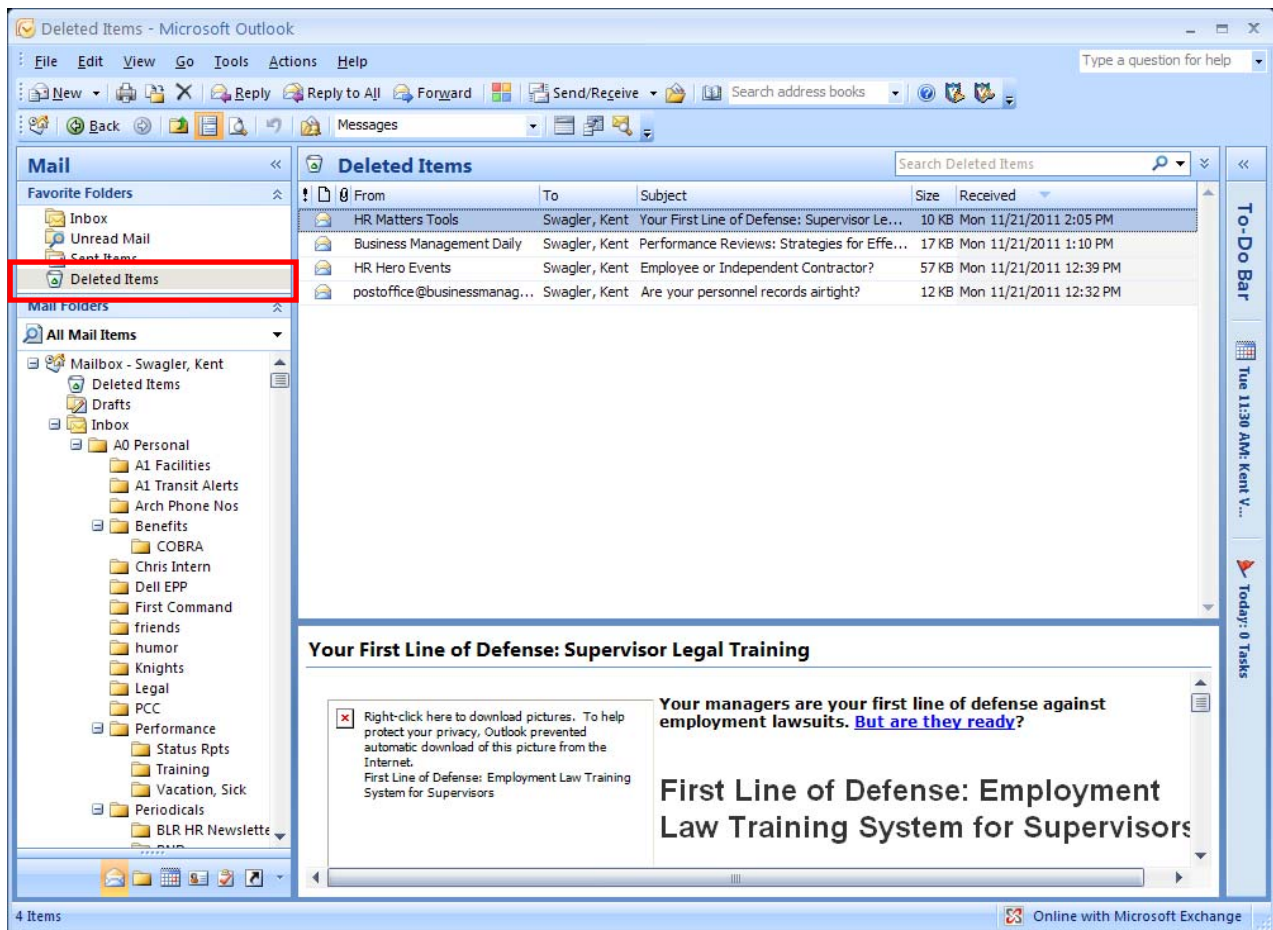
EMAIL RECORDS MANAGEMENT

Storing Business Emails

All personal and non-business related emails and electronic documents must be deleted as soon as they are read. All other business-related emails should be filed in a folder in accordance with your department/division's file plan.

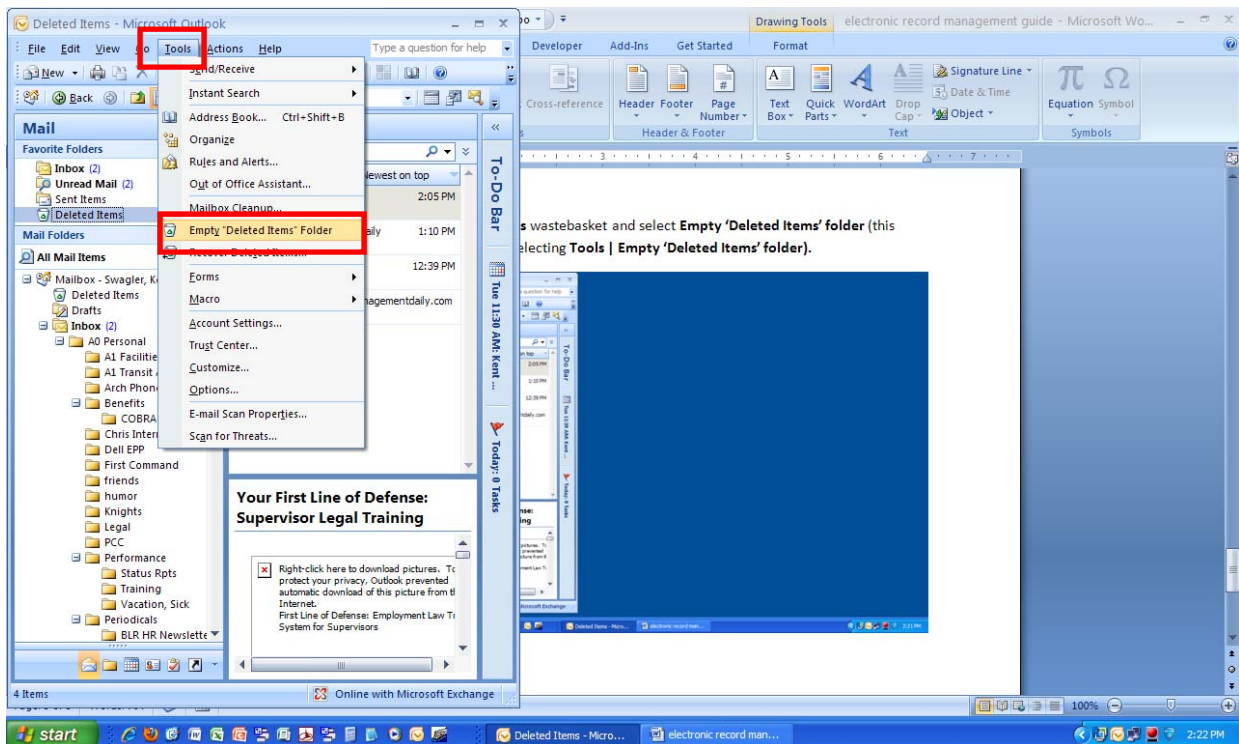
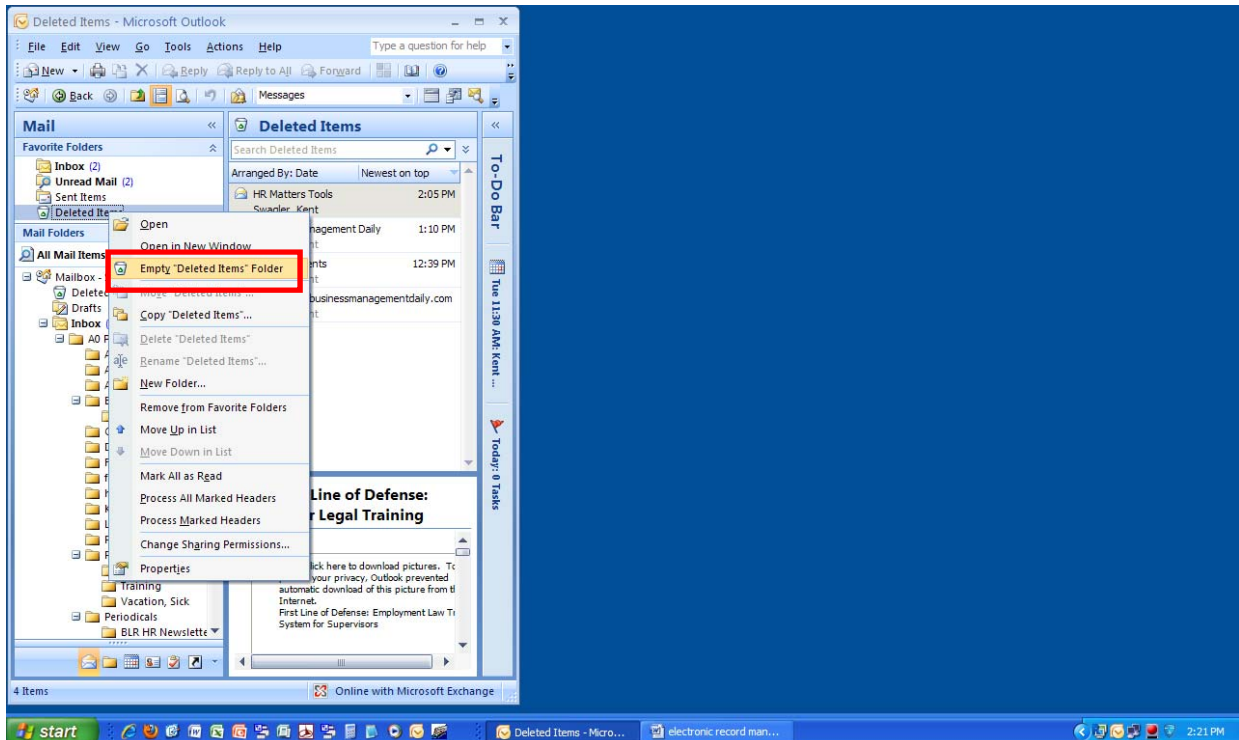
Deleting Emails

Deleting email does not automatically destroy it from your email account. Deleting places it into your **Deleted Items** wastebasket. This allows you to recover any emails you accidentally delete by moving it to your Inbox or one of your email folders.



Emptying the Wastebasket

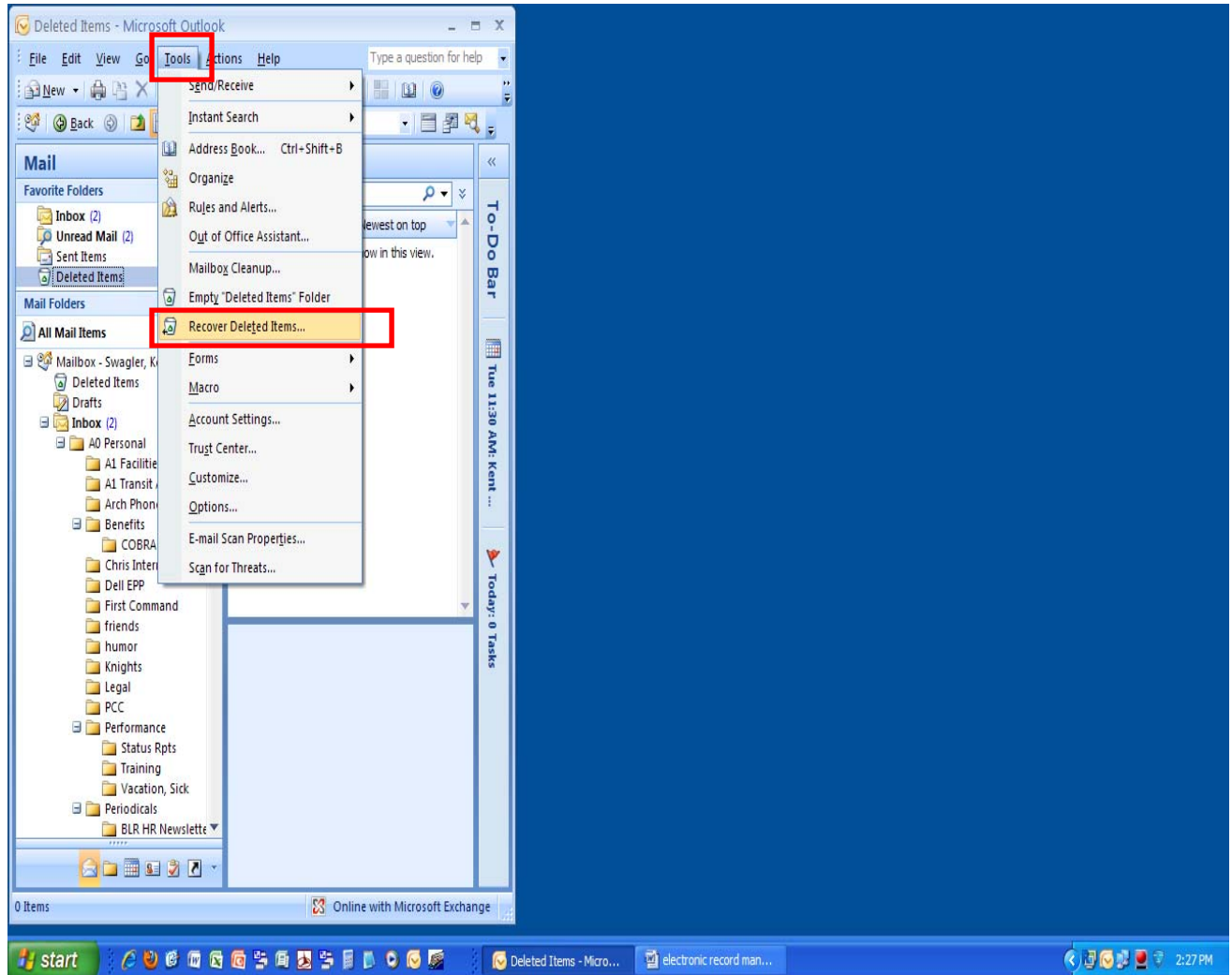
Right-click on the **Deleted Items** wastebasket folder and select **Empty 'Deleted Items' folder** (this command is also available by selecting **Tools | Empty 'Deleted Items' folder**). Click the **Yes** button. All items are deleted from your wastebasket.



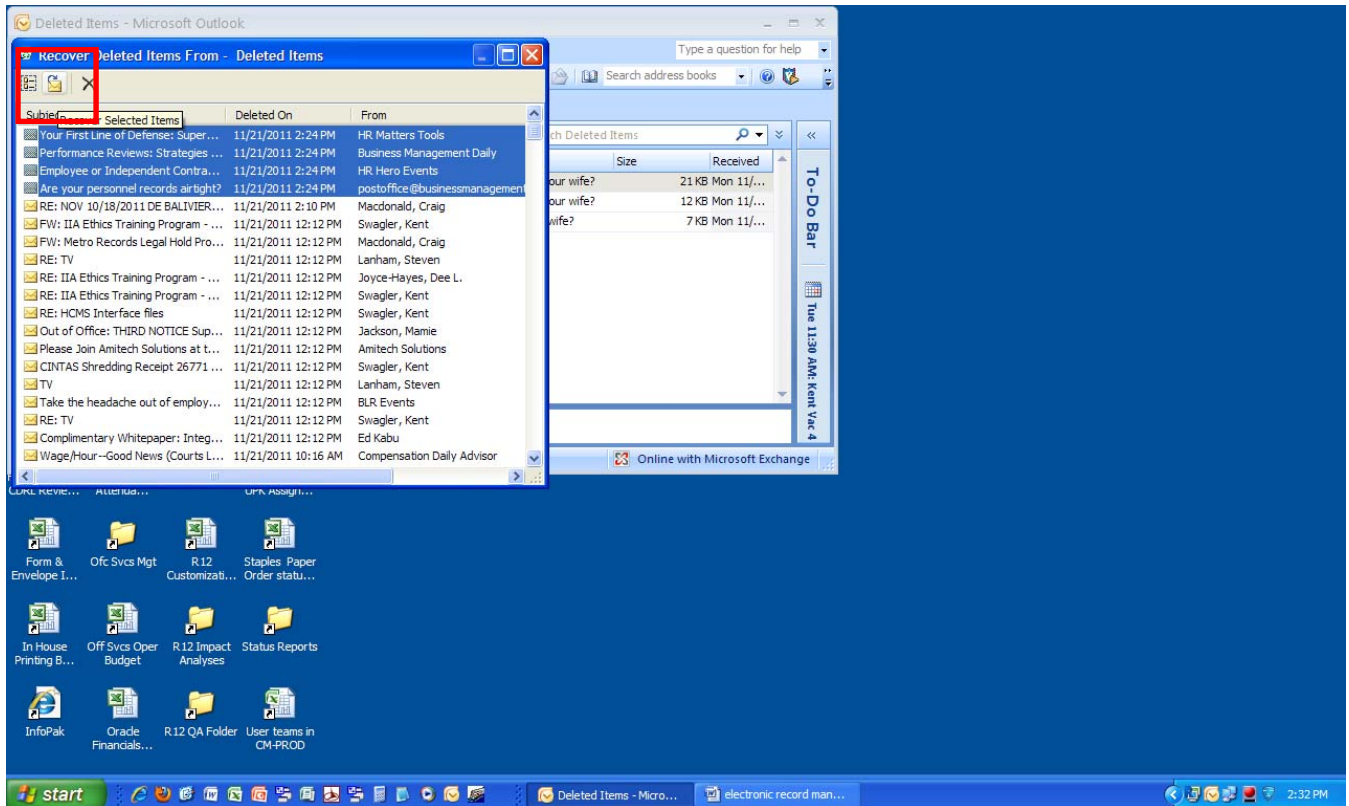
Recovering Emails Deleted from the Wastebasket

If emails were accidentally deleted from both your email folder(s) and your Wastebasket,

1. Select **Tools | Recover Deleted Items . . .**



2. Highlight the emails you want to restore and click on the **Recover Selected Items** icon. The emails will be restored to their previous location.



Please note: There is a seven-day retention period for all emails deleted from your wastebasket. If you need to recover emails or files that were deleted longer than seven days ago, contact the Help Desk (extension 5555) to submit a file recovery request.

Archiving Email Folders

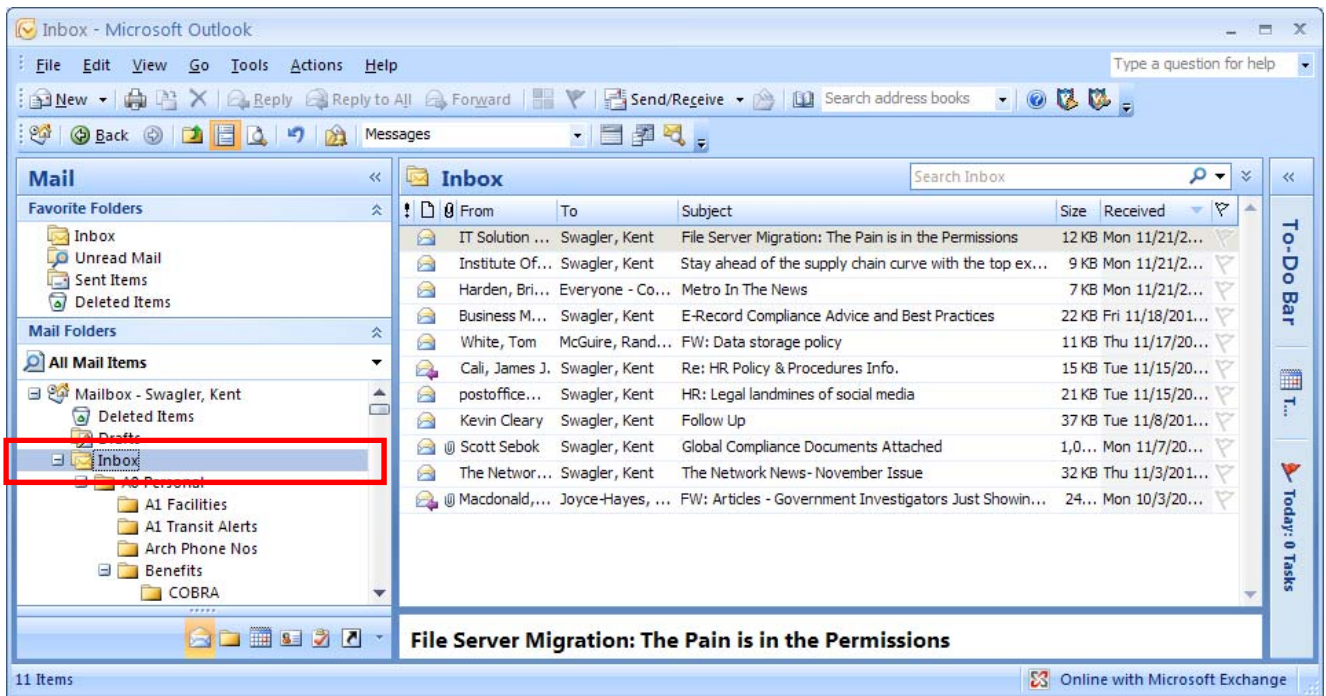
Due to the high volume of emails sent and received every day, some with large file attachments, all email accounts have a default storage limit of 55 megabytes (MB) assigned to them. Even with the best email cleanup efforts, the volume of business-related emails that need to be retained per the Records Retention Policy can sometimes exceed the mailbox size limit.

To off-load your primary email box, older emails can be archived to a separate mailbox folder that is typically stored on your U:\ (User) network drive for security and to ensure that it is backed up every day.

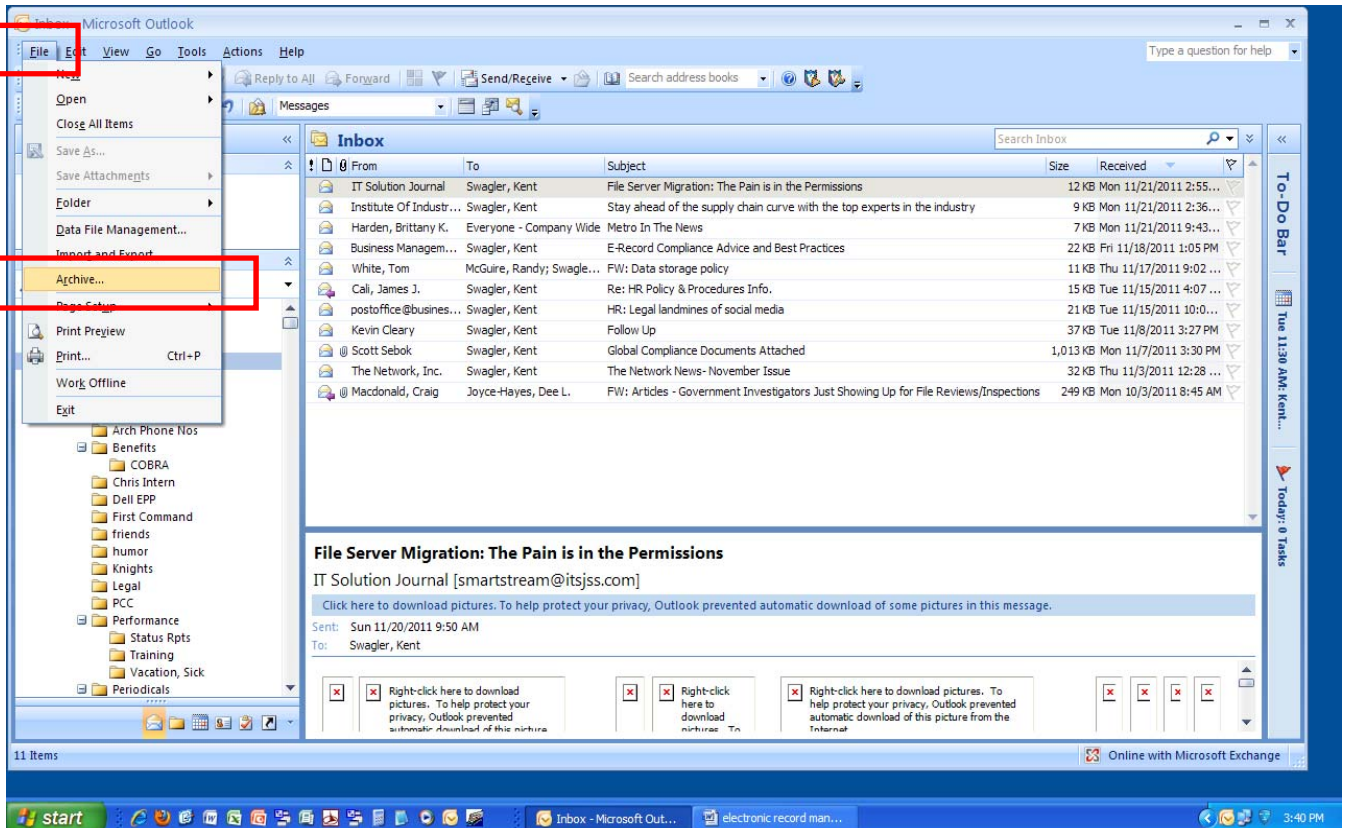
*Before beginning the archive process, clean your email folders of any emails that are no longer needed, including emptying the **Deleted Items** wastebasket folder.*

To create a new email archive folder:

1. Click on the **Inbox** to make sure it is highlighted

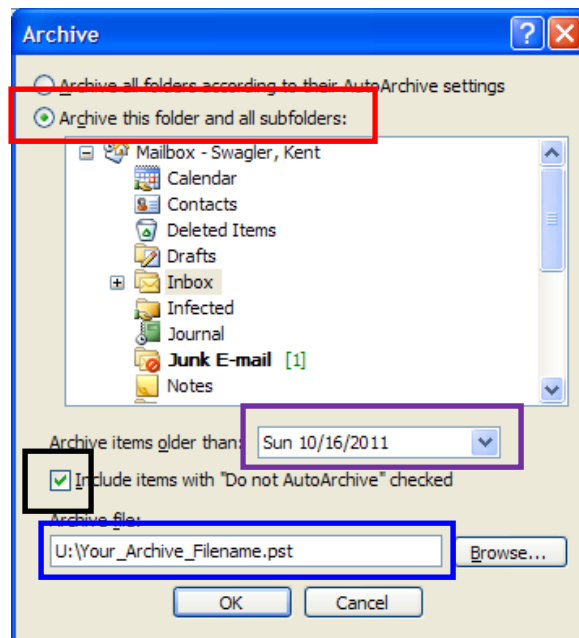


2. Select **File | Archive**

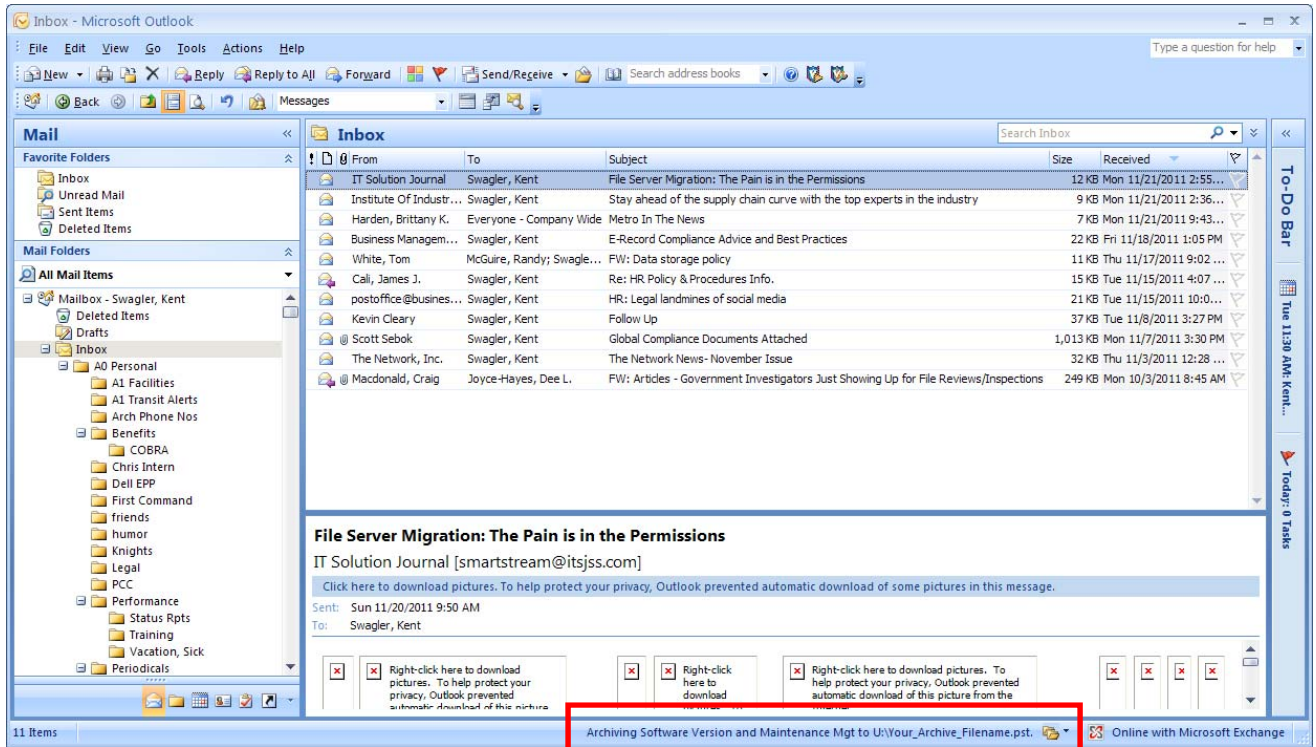


3. Complete the following actions:

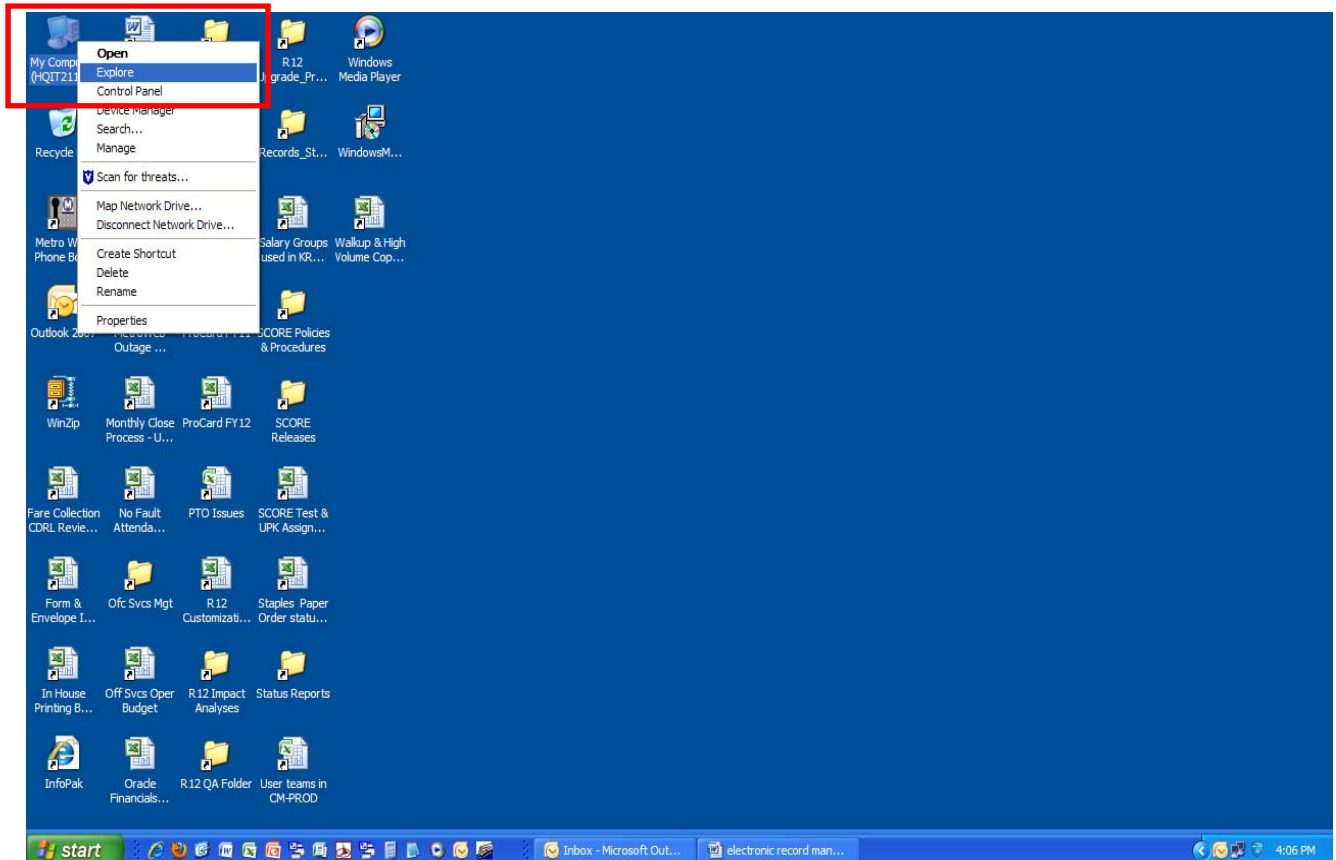
- a. Make sure the **Archive this folder and all subfolders** radio button is filled in;
- b. Select a date to **Archive items older than** the selected date (recommend selecting 30 days before the current date);
- c. Make sure the **Include items with "Do not AutoArchive" checked** checkbox is filled in;
- d. Change the **Archive file** name to from the default name to a new name. Make sure the file extension is still **.pst**. Click the **OK** button.



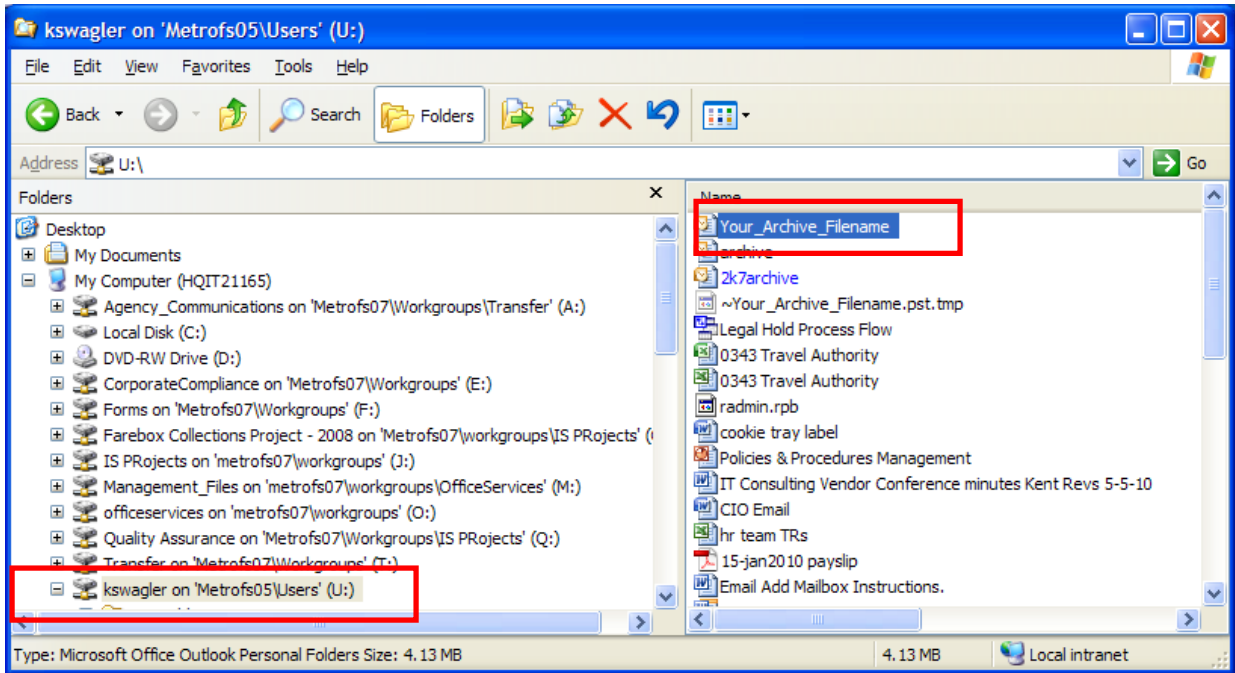
The archive process will begin and usually takes several minutes to complete the first time it is run. When it is processing, status messages are displayed at the bottom of the window.



4. When it is completed, open Windows Explorer by right-clicking on the **My Computer** icon and select **Explore**



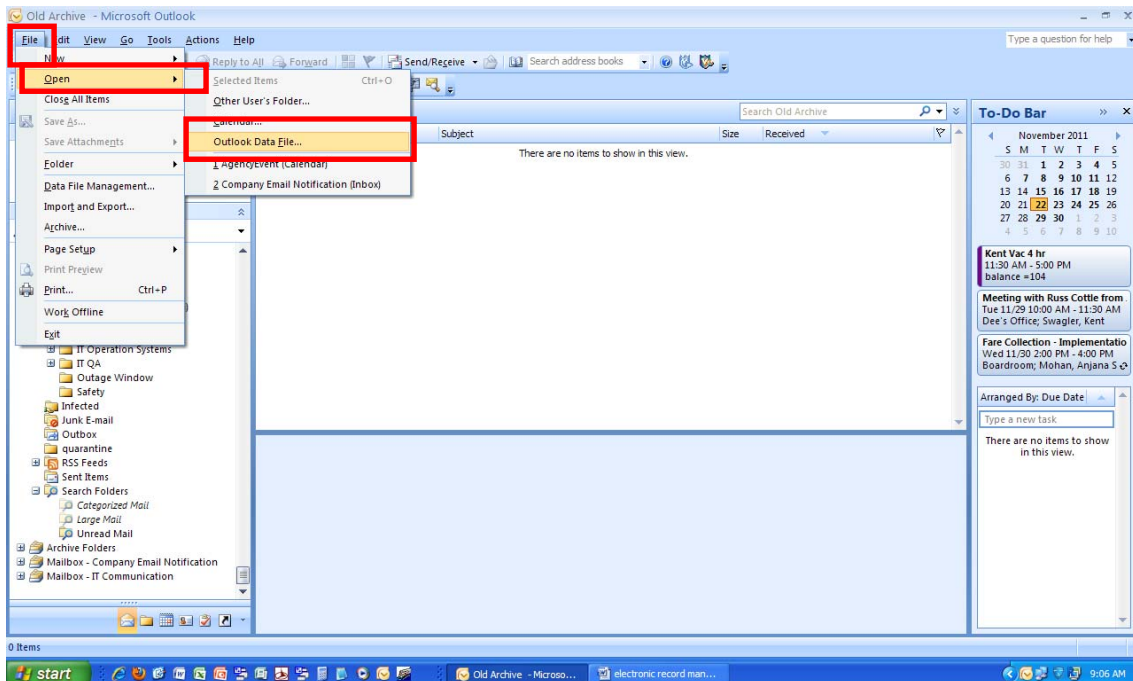
5. Click on the U:\ drive and the new archive file is now on the drive.



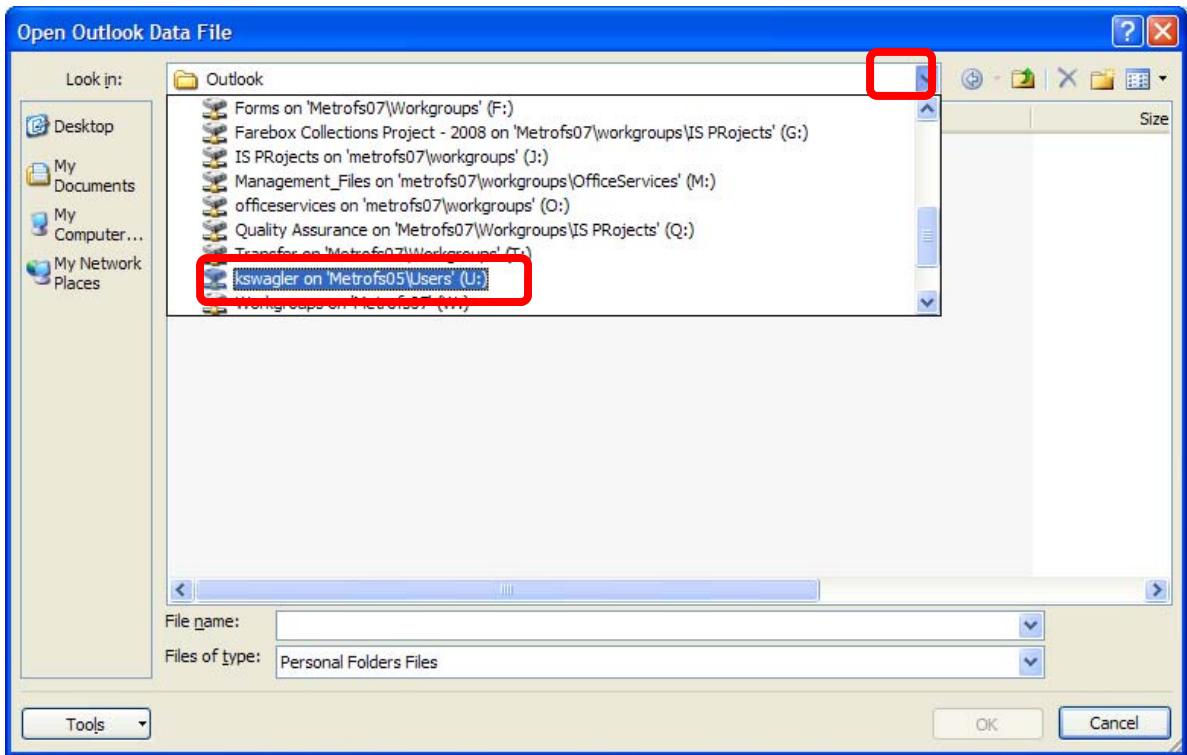
Accessing your Email Archive Folder through Email

Eventually, emails stored in your archive file will expire and must be deleted. To access your archive folder for easier review and deletion, you will need to set up a link to your archive folder in your email folder list. The steps to set up a link are listed below:

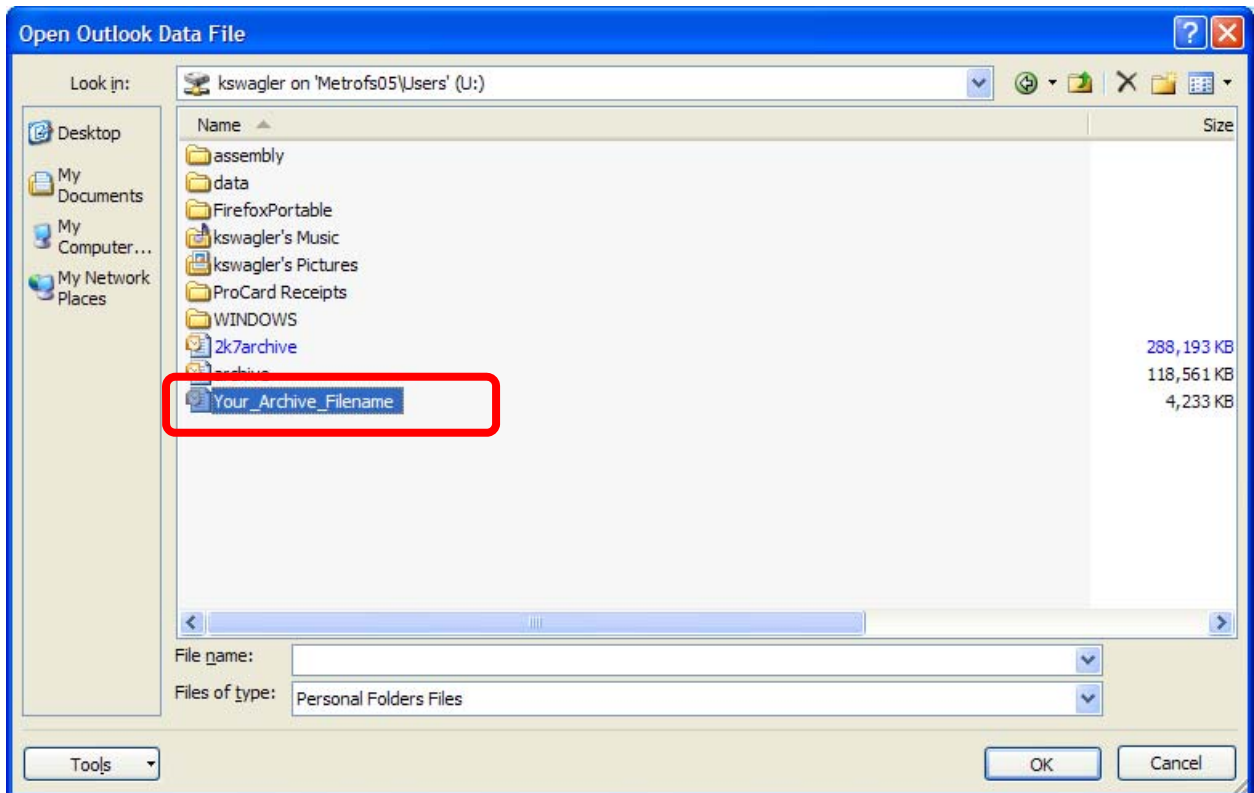
1. Select **File | Open | Outlook Data File . . .**



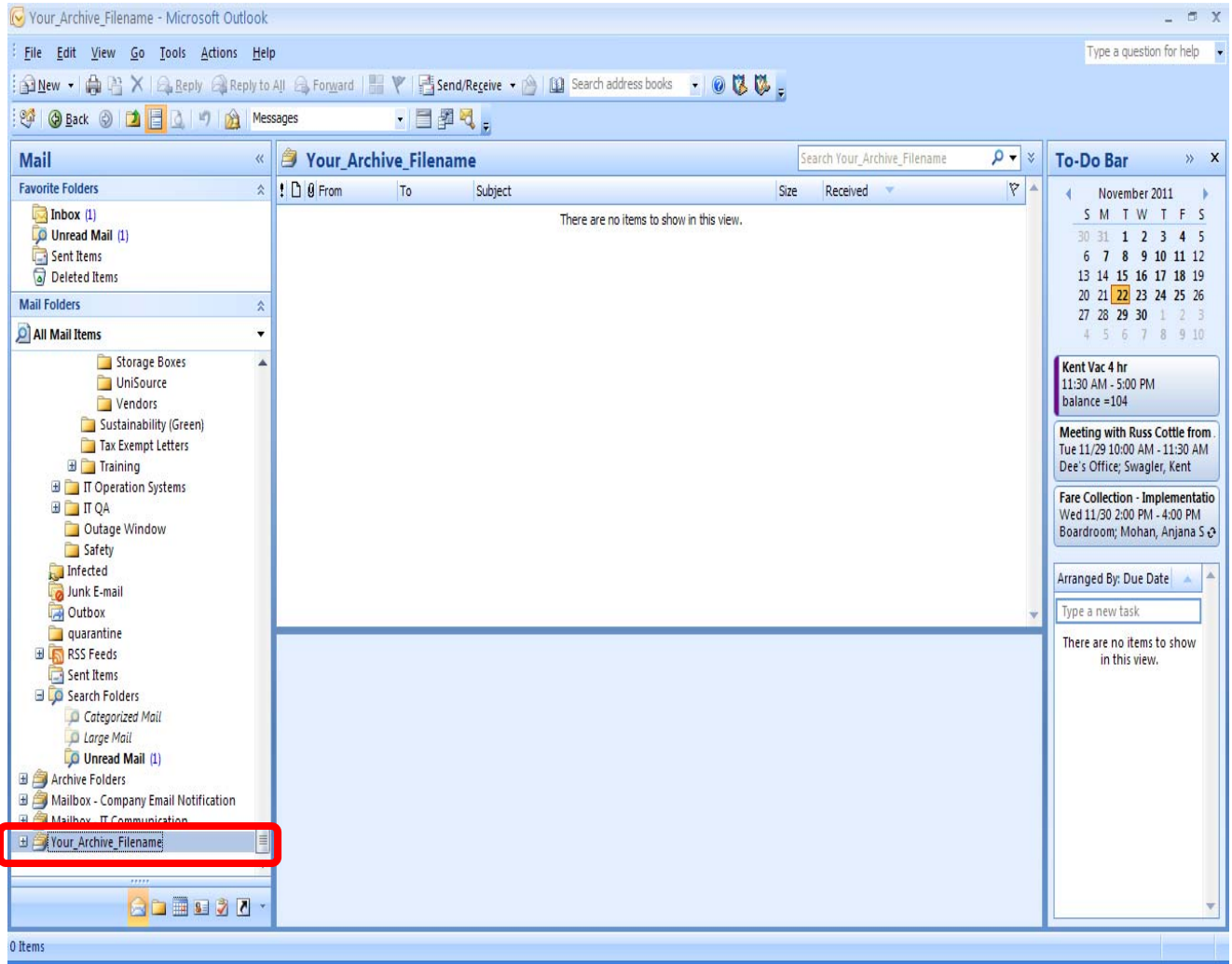
2. Click the dropdown selection arrow and click on your U:\ network drive.



3. Highlight the new archive file you just created and click the **OK** button.



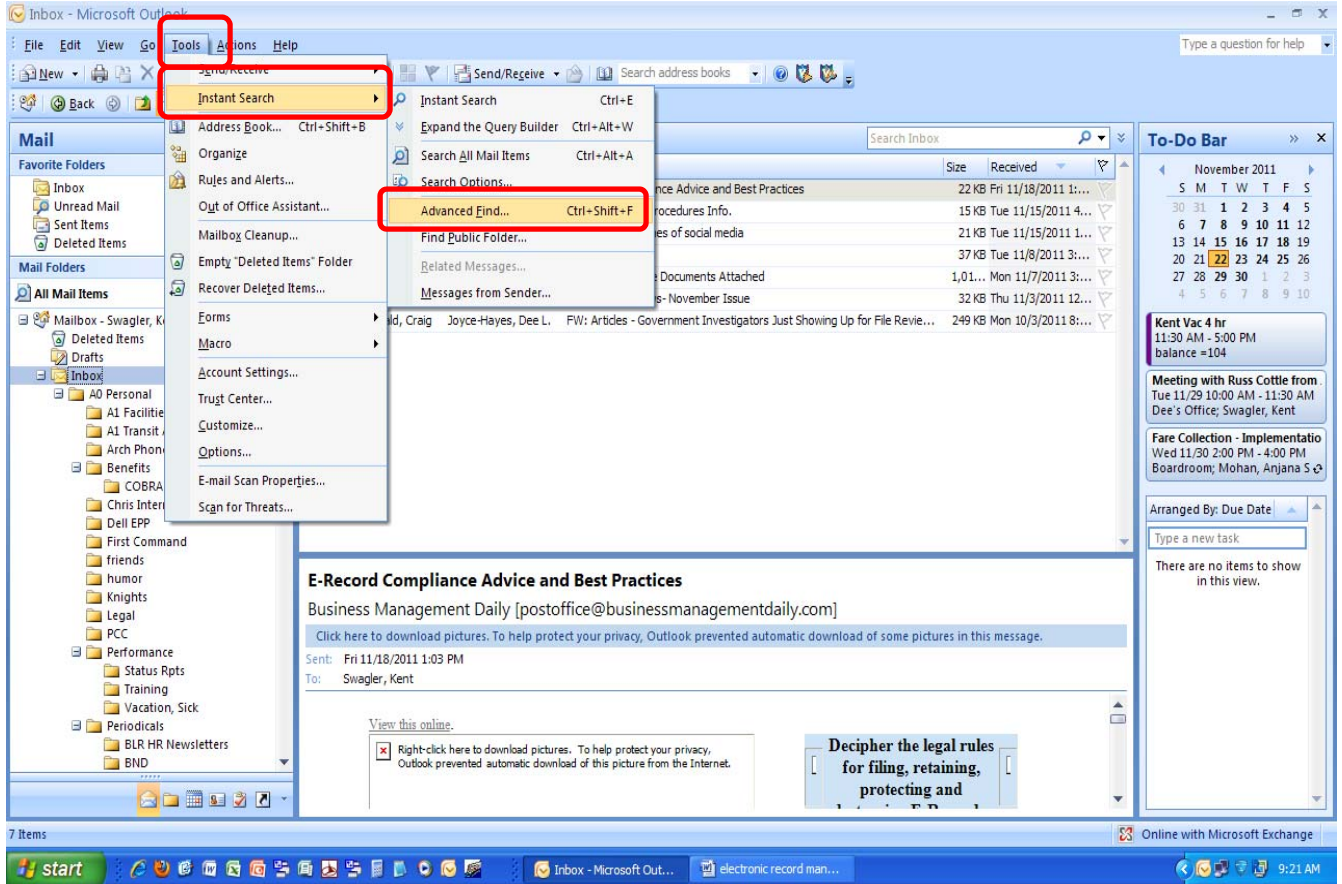
- The archive file is now listed at the bottom of your Email Folder list. Click on the + expand button to display all your email folders that were archived.



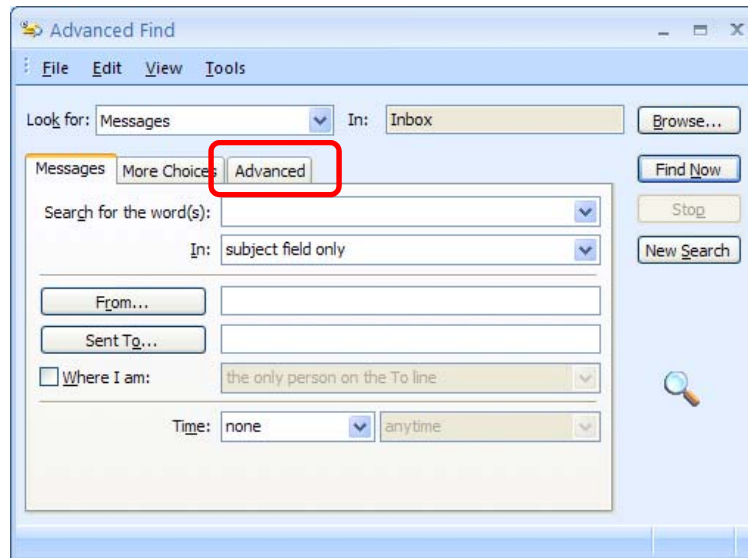
Searching for Expired Emails – Active Inbox and Archive Email Folders

To search your active inbox for expired emails:

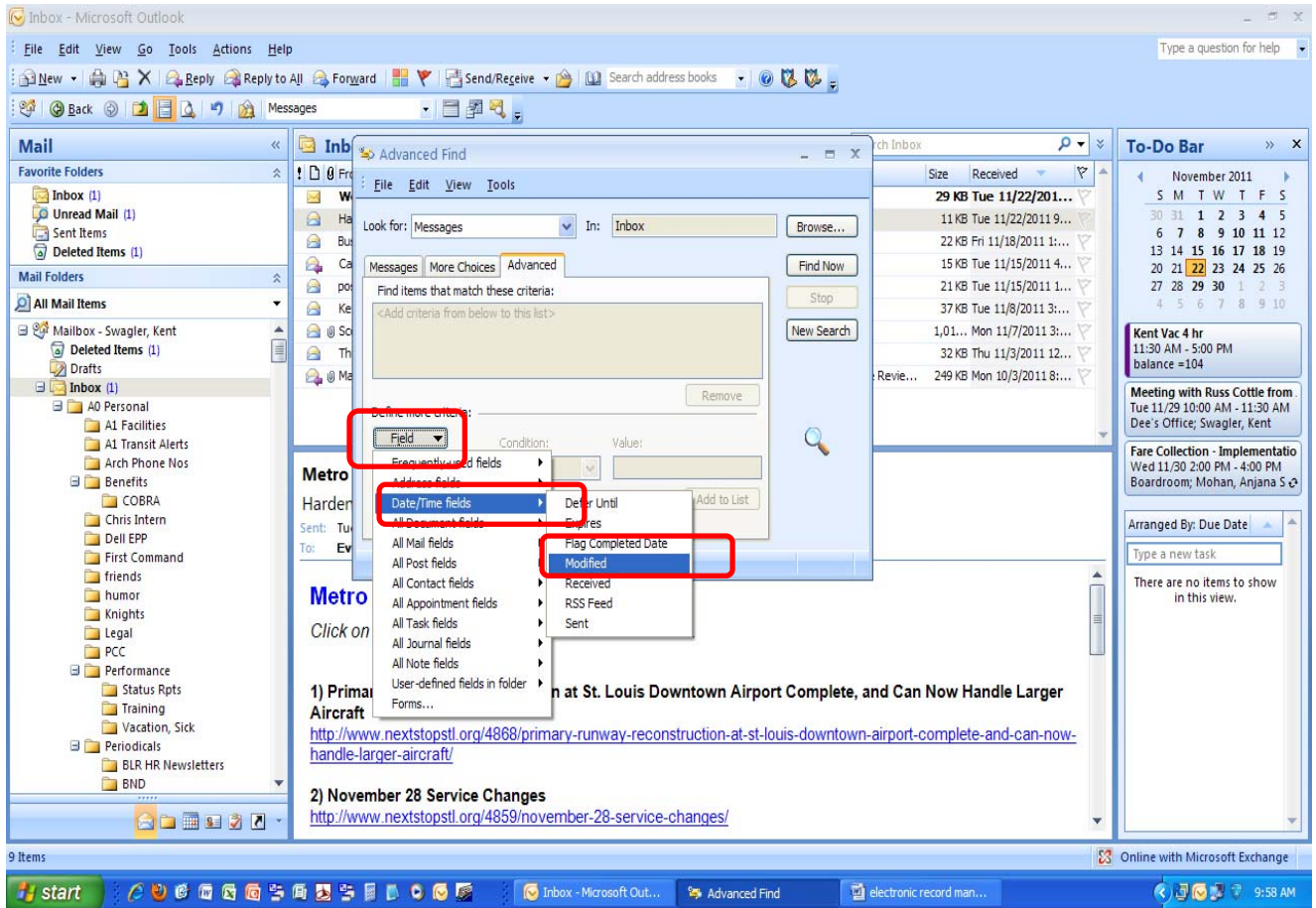
1. Highlight your inbox and select **Tools | Instant Search | Advanced Find . . .**



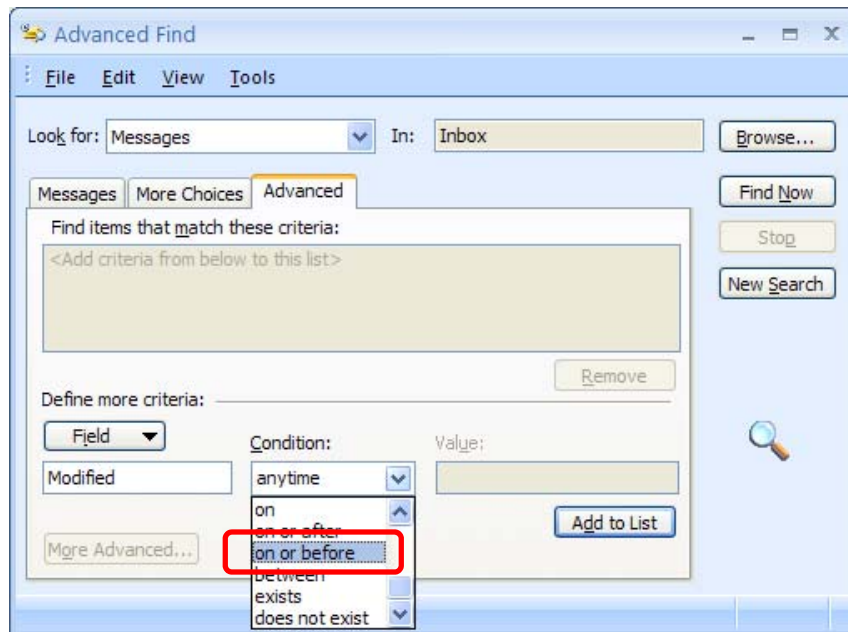
2. Click the **Advanced** tab



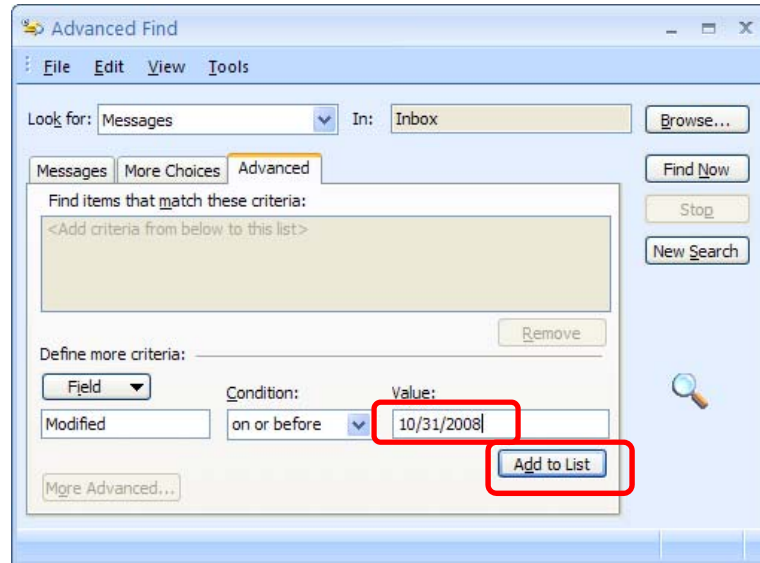
3. In the **Field** dropdown menu, select **Date/Time Fields | Modified**



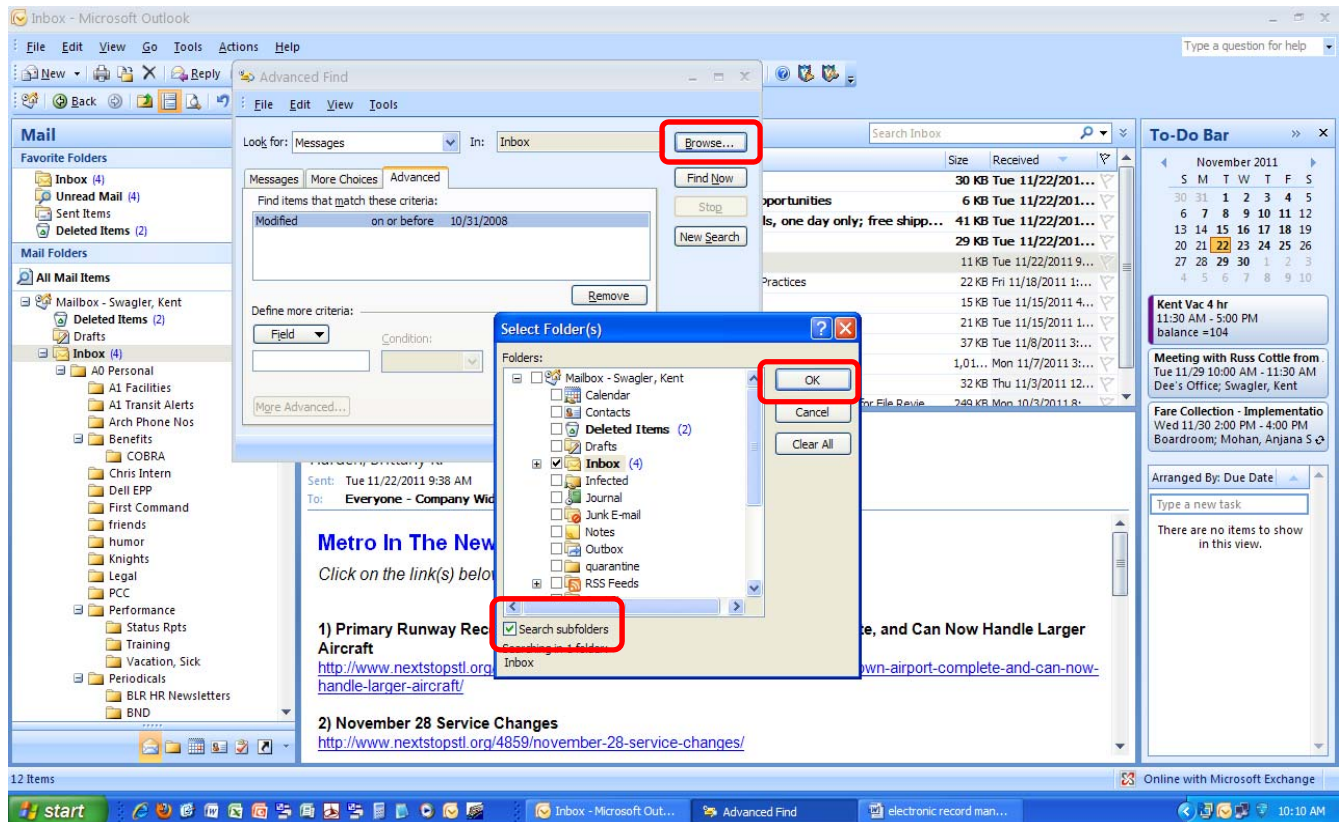
4. In the **Condition** dropdown, select **on or before**



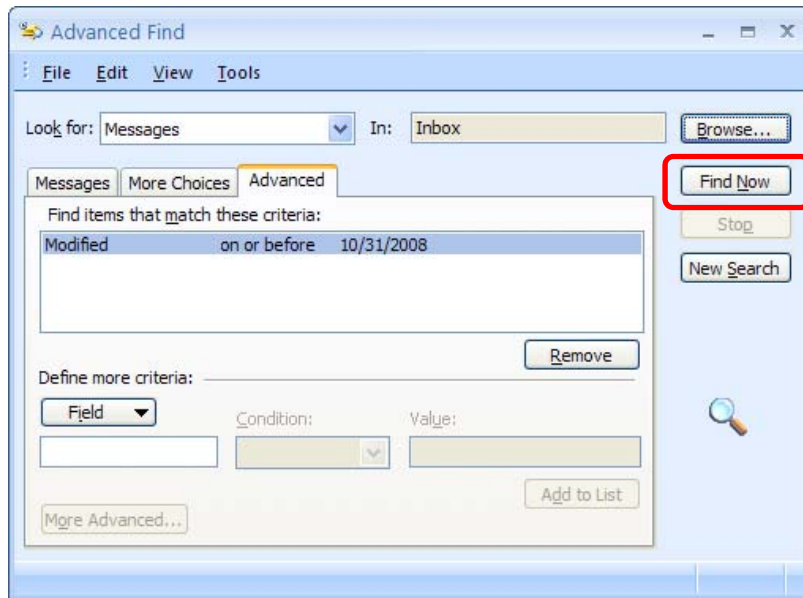
5. In the **Value:** field, enter a date where emails that are older than that date have expired in the format DD/MM/YYYY. For example, if you are looking for emails that you needed to retain for three years and today's date is November 1, 2011, then enter the date **10/31/2008** and click the **Add to List** button.



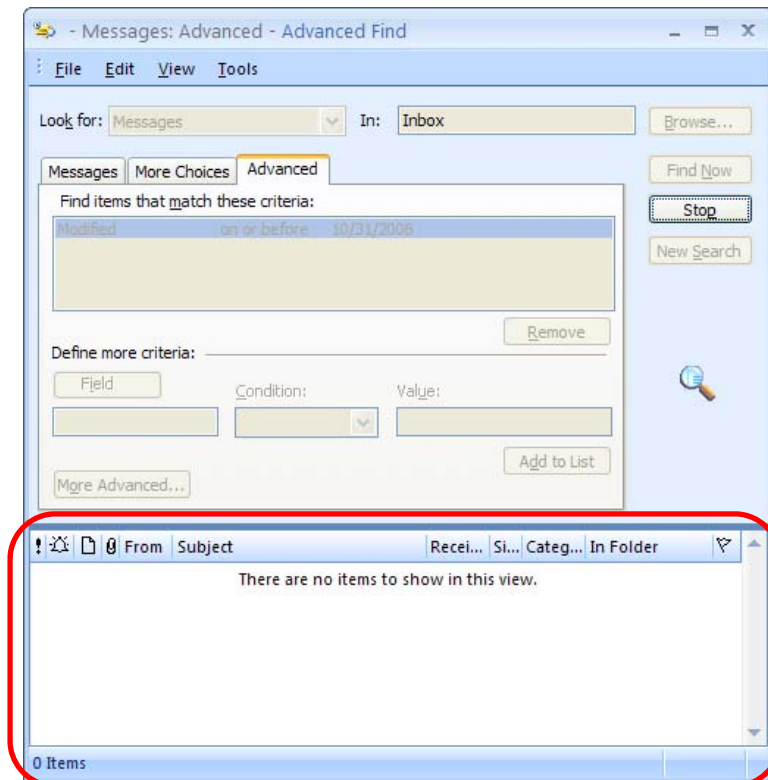
6. To have all folders and subfolders searched in your Inbox, click the **Browse** button, make sure the Inbox is highlighted, fill the **Search subfolders** checkbox, and click the **OK** button.



7. When the Select Folder(s) window disappears, click the **Find Now** button.



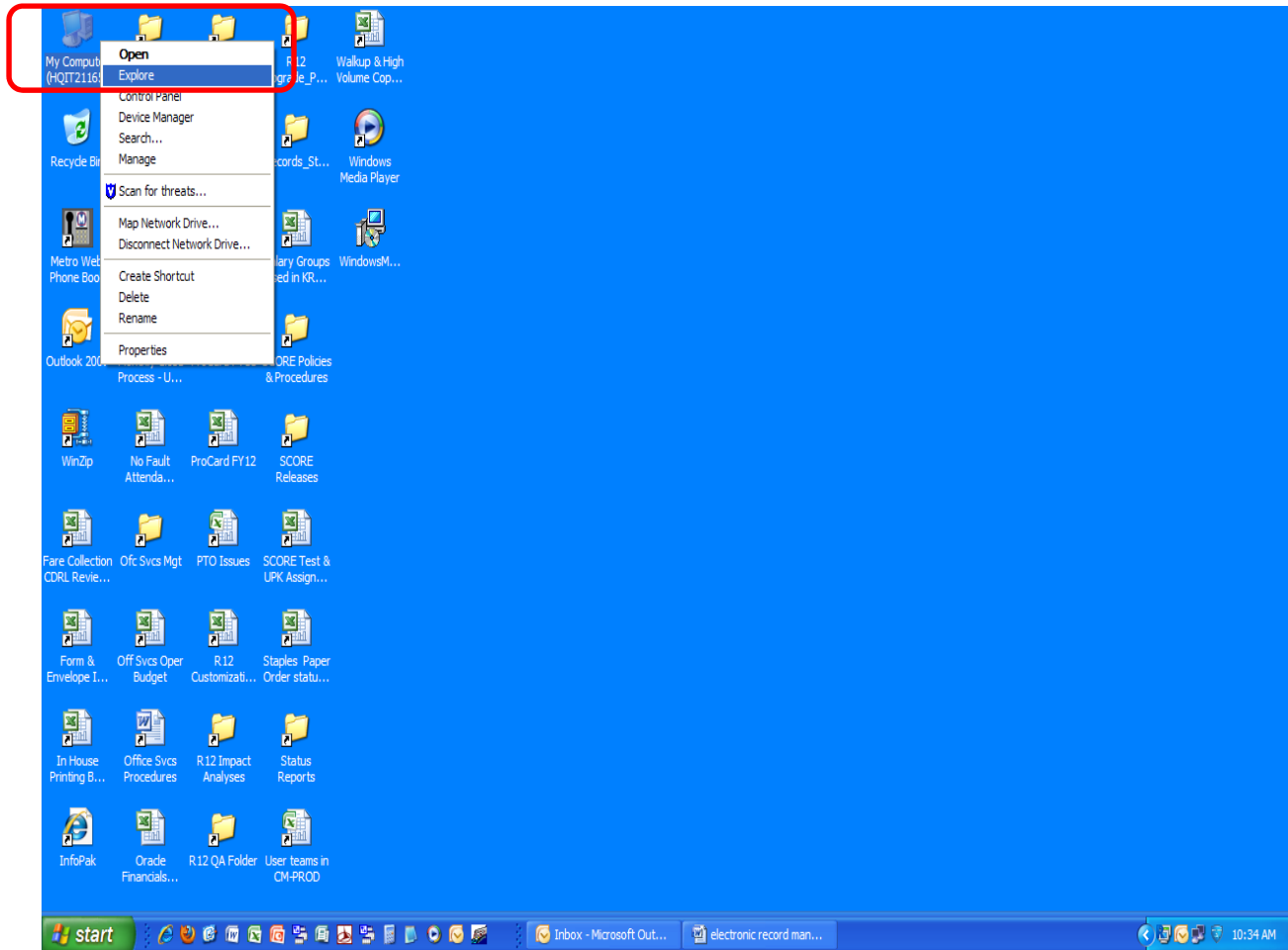
8. The search begins and any emails meeting your search criteria will be listed in the results area. The emails listed can be reviewed and deleted.



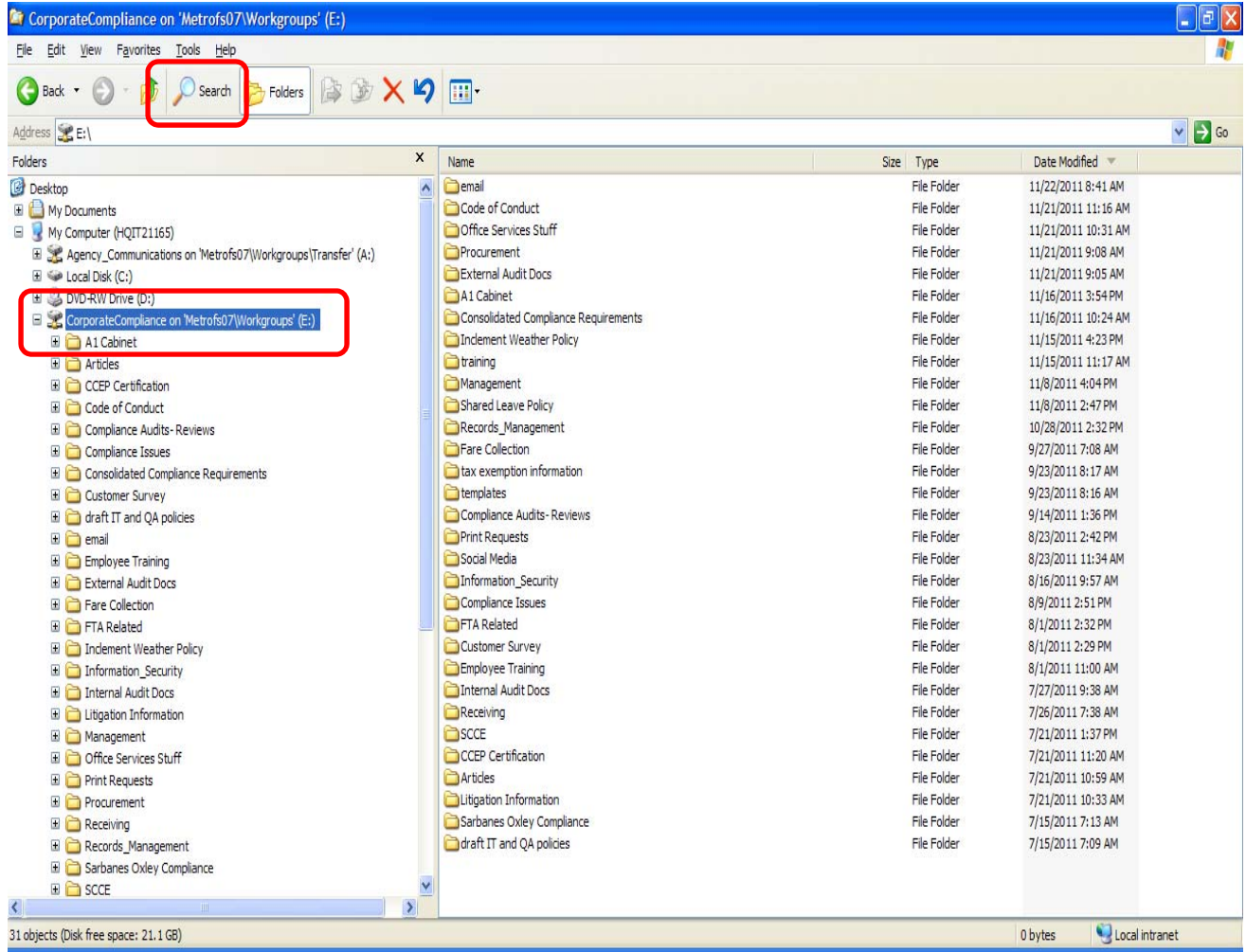
To search for expired emails in your Archive folder, scroll down to your archive folder and repeat steps 1-8 above.

Searching for Expired Electronic Files in Network Drive Folders

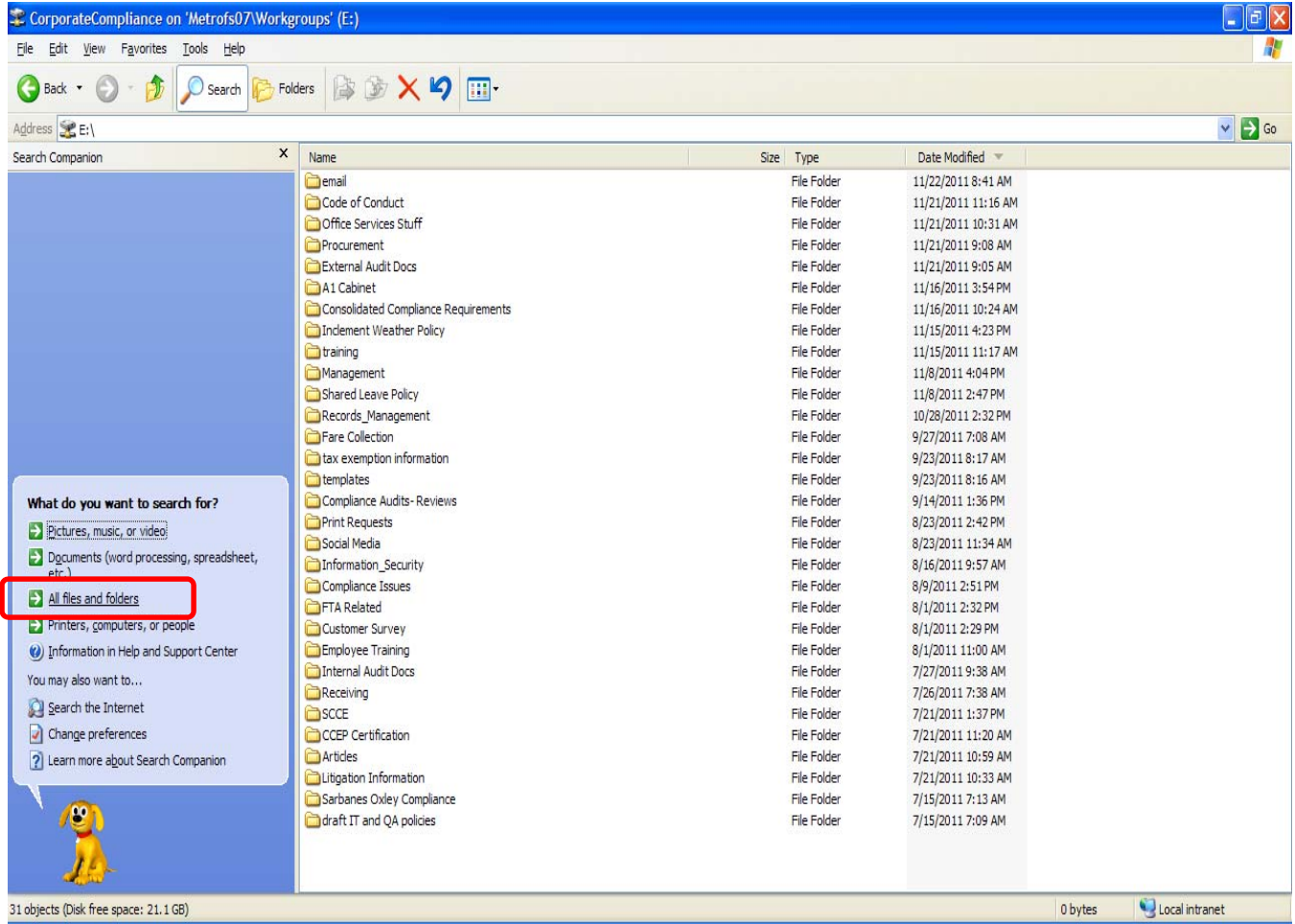
1. Right-click on the My Computer desktop icon and select **Explore**.



2. Highlight the network drive and folder you want to search and click the **Search** button.

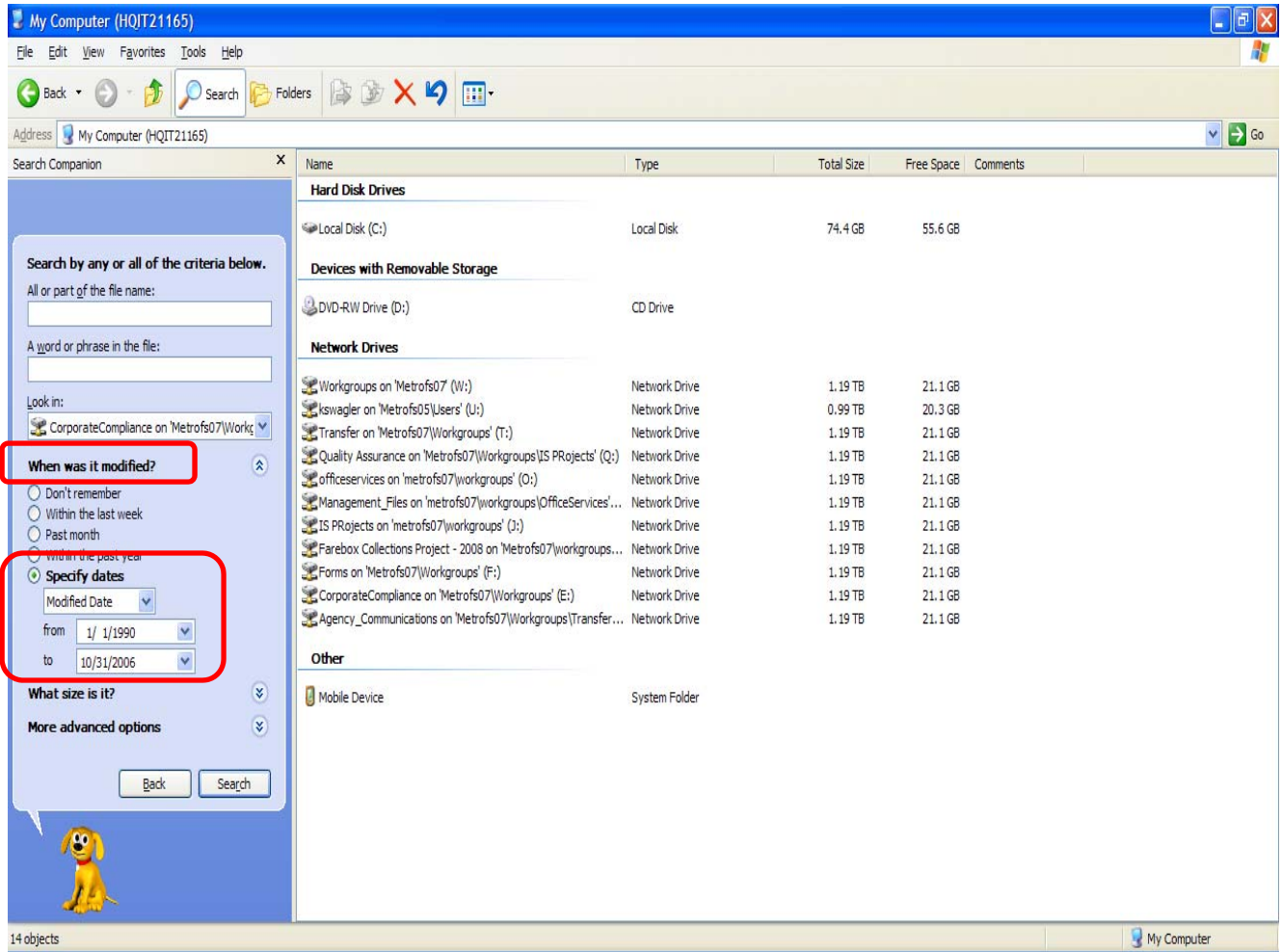


3. Click on the **All Files and Folders** option



- Click on **When was it modified?**, fill in the Specify dates radio button, and enter a **from** and **to** date range for any records that have expired.

For example, if this is the first time you are searching, and you are looking for records that are older than five years from the current date of November 1, 2011, enter a **from** date of **1/1/1990** and a **to** date of **10/31/2006**.



- The search begins and any files meeting your search criteria will be listed in the results area. The files listed can be reviewed and deleted.

Please note: If files were accidentally deleted on a network folder or drive, you must contact the IT Help Desk to submit a file recovery request.

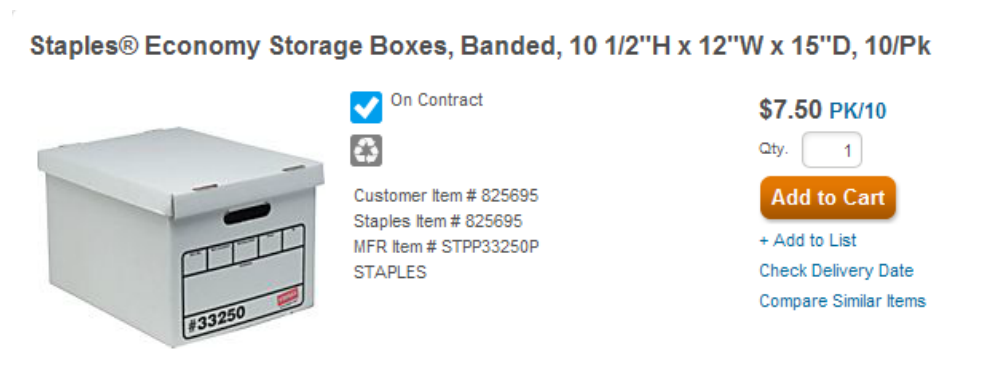
***Procedure for Preparing Inactive Hard Copy Records
(microfilm and microfiche are not accepted for storage)***

1. Once inactive records have passed the retention period for departmental storage as outlined in the Records Retention Schedule outlined in the Metro Records Retention Policy, contact the Metro Director of Corporate Compliance (who is the Agency's Records Administrator) for transfer to the Records Center. The Corporate Compliance Director will assign a control number for these records and email Metro Form 0209, Records Transmittal and a copy of these procedures.

The Corporate Compliance Director assigns the next available control number maintained in current calendar year spreadsheet (located at **w:\CorporateCompliance\records management\Records_Storage_Index\Records Storage Index 20XX - .xlsx**). The Control number format is YYYYXX where YYYY is current calendar year and XX is incremental number assigned. Each control number is only used once.

To keep all boxes stored together in the same storage area, no more than 20 boxes are assigned to one control number. If a new group of records is transferred later in the future, a new control number will be assigned.

2. Order the standard size records storage boxes from the current Metro Office Supply vendor (currently Staples). Detailed information is provided below:



The screenshot shows a product listing for Staples Economy Storage Boxes. The title is "Staples® Economy Storage Boxes, Banded, 10 1/2\"H x 12\"W x 15\"D, 10/Pk". Below the title is a photograph of a white storage box with a label that includes the number "#33250". To the right of the image are several icons and text: a blue checkmark icon with "On Contract", a recycling icon, and the text "Customer Item # 825695", "Staples Item # 825695", "MFR Item # STPP33250P", and "STAPLES". Further right, the price is listed as "\$7.50 PK/10", followed by a quantity selector set to "1", an orange "Add to Cart" button, and links for "+ Add to List", "Check Delivery Date", and "Compare Similar Items".

3. These boxes were selected based on their price, size, and durability. **Any other box for records storage will not be accepted.** The contents of one box are equivalent to half a file drawer or less.
4. When packing the boxes:
 - a. Remove all hanging folders, as they damage the sides of the storage box.
 - b. Pack the box no more than 90% full, as the box handles can still be used for carrying.
 - c. Document the contents of each box in the transmittal form. The amount of detail used when indexing the records should be sufficient for locating the record to retrieve it later.

- d. Tape the lids to the box to avoid losing the contents during transport in the truck.
- e. Using a marker, label the box at the foot or head (not the sides, top, or bottom) with the following information:
 - i. Department or cost center name
 - ii. General description of the records
 - iii. From-To dates of records
 - iv. Destruction Date (see Master Records Retention Schedule)
 - v. Control Number
 - vi. Box number (example: 1 of 4, 2 of 4, 3 of 4, 4 of 4)

Please note: Whole-sheet box labels are available from the Office Services High Volume Print Center by submitting a Metro Form 0066 Duplicating Request to print copies of Metro Form 0065 Records Storage Box Label. These forms as well as all other Metro forms can be found at [w:\forms](#).

- f. When all the boxes are prepared according to these procedures and the Records Transmittal form is completed, email the form to the Corporate Compliance Director.
 - g. The Corporate Compliance Director will arrange for pick-up and will assign a location number to each box.
5. The Corporate Compliance Director sends email to Agency Courier (Charlie Priscu for all Bus facility and Headquarters records, Leroy Coonce / Steve Brasfield for all Rail facility records) to pick up boxes and deliver them to:
 - a. Illinois Bus Facility – for all records owned by Headquarters and Illinois facilities
 - b. Brentwood Bus Facility – for all records owned by Missouri facilities.
 6. The storage life is dependent on records retention period stated in the box list and on each box and is reviewed against the current published version of the Metro Records Retention Policy.

Procedure for Retrieving Inactive Records

1. Email a retrieval request to the Corporate Compliance Director. Indicate the Control Number and Box Number(s) as referenced by the Records Transmittal originally sent by the requesting department. If the requesting department is unable to locate this information, the Corporate Compliance Director should be contacted for assistance.
2. The Corporate Compliance Director then sends retrieval request to Agency Courier to pick up desired boxes and deliver them to requestor's location
3. For microfilmed or microfiched records, the requester is responsible for storing, viewing, and copying records, including obtaining viewing and copying equipment from external sources.
4. Requesters may only have access to records generated from their departments. Records not originated from their departments must be requested through the owner department.

FROM:

SPACE NO. _____

RECORD DESCRIPTION:

DATES ENCLOSED:

ESTIMATED DESTRUCTION DATE:
(To be revisited before destroying)

FROM: _____ **TO:** _____

CONTROL NO. _____

BOX NO. _____ **OF** _____

Abuse of or Fraud with Company Benefits (Employee Benefits Abuses)**CHANGE**

Name	Title	Primary	Email
	Director Benefits	Yes	Yes
	General Counsel	Yes	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Human Resources	No	Yes

Accounting and Auditing Matters**CHANGE**

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Senior Vice President & Chief Financial Officer	No	Yes
	Director of Corporate Compliance	Yes	Yes

Accurate Books & Records**CHANGE**

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes

Confidentiality and Misappropriation**CHANGE**

Name	Title	Primary	Email
	Vice President & CIO	No	Yes
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes

Conflict of Interest**CHANGE**

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director of Corporate Compliance	Yes	Yes

Contractor/Vendor Relations CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Procurement & Inventory Mgt	No	Yes

Data Privacy CHANGE

Name	Title	Primary	Email
	Vice President & CIO	Yes	Yes
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes

Disclosure of Confidential Information CHANGE

Name	Title	Primary	Email
	Vice President & CIO	No	Yes
	General Counsel	Yes	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Human Resources	No	Yes

Discrimination or Harassment CHANGE

Name	Title	Primary	Email
	General Counsel	No	Yes
	Director of Corporate Compliance	No	Yes
	Director Workforce Diversity & EEO	Yes	Yes

Embezzlement CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Senior Vice President & Chief Financial Officer	No	Yes
	Director of Corporate Compliance	Yes	Yes

Environmental Protection, Health or Safety Law CHANGE

Name	Title	Primary	Email
	Director Risk Management, Safety, & Claims	No	Yes
	General Counsel	Yes	Yes
	Senior Vice President & Chief Financial Officer	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Senior Vice President Operations	No	Yes

False Healthcare Claims CHANGE

Name	Title	Primary	Email
	Director Benefits	Yes	Yes
	General Counsel	No	Yes
	Director of Corporate Compliance	No	Yes
	Vice President Human Resources	No	Yes

Falsification of Contracts, Reports or Records CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Procurement & Inventory Mgt	No	Yes

Government Contracts CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Procurement & Inventory Mgt	No	Yes

Health Insurance Portability and Accountability Act CHANGE

Name	Title	Primary	Email
	Director Benefits	Yes	Yes
	General Counsel	No	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Human Resources	No	Yes

High Priority Threat CHANGE

Name	Title	Primary	Email
	General Counsel	No	Yes
	Director of Corporate Compliance	No	Yes
	Senior Vice President Operations	No	Yes

Hiring Irregularities CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Human Resources	No	Yes

Improper Giving or Receiving of Gifts CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Procurement & Inventory Mgt	No	Yes

Improper Supplier or Contractor Activity CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Procurement & Inventory Mgt	No	Yes

Misuse of Assets or Services CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes

Neptism/Favoritism Inappropriate Workplace Relationships CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Director Workforce Diversity & EEO	No	Yes

Offensive or Inappropriate Communication CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director of Corporate Compliance	Yes	Yes
	Director Workforce Diversity & EEO	No	Yes

Retaliation CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director of Corporate Compliance	Yes	Yes
	Director Workforce Diversity & EEO	No	Yes

Safety CHANGE

Name	Title	Primary	Email
	Director Risk Management, Safety, & Claims	No	Yes
	General Counsel	Yes	Yes
	Senior Vice President & Chief Financial Officer	No	Yes
	Director of Corporate Compliance	Yes	Yes

Sexual Harassment CHANGE

Name	Title	Primary	Email
	General Counsel	No	Yes
	Director of Corporate Compliance	No	Yes
	Director Workforce Diversity & EEO	Yes	Yes

Stimulus Act Abuse CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Senior Vice President & Chief Financial Officer	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Vice President Procurement & Inventory Mgt	No	Yes

Substance Abuse CHANGE

Name	Title	Primary	Email
	Director Risk Management, Safety, & Claims	No	Yes
	General Counsel	Yes	Yes
	Senior Vice President & Chief Financial Officer	No	Yes
	Director of Corporate Compliance	Yes	Yes

Theft CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Chief of Security/Fare Enforcement	No	Yes

Threat or Inappropriate Supervisor Directive CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director, Labor Relations	No	Yes
	Director of Corporate Compliance	Yes	Yes
	Director Workforce Diversity & EEO	No	Yes

Time Abuse CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Senior Vice President & Chief Financial Officer	No	Yes
	Director of Corporate Compliance	Yes	Yes

Unsafe Working Conditions CHANGE

Name	Title	Primary	Email
	Director Risk Management, Safety, & Claims	No	Yes
	General Counsel	Yes	Yes
	Senior Vice President & Chief Financial Officer	No	Yes
	Director of Corporate Compliance	Yes	Yes

Violation of Policy CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes

Workplace Violence CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director of Corporate Compliance	Yes	Yes
	Chief of Security/Fare Enforcement	No	Yes

Other CHANGE

Name	Title	Primary	Email
	General Counsel	Yes	Yes
	Director	No	Yes
	Director of Corporate Compliance	Yes	Yes

Fraud and Ethics Hotline and Case Management Services - Cost Evaluation

Recurring Annual Costs

7.1 Annual Fees

7.1.1 Incident reporting: Fees can be quoted as:

7.1.1.1 Cost Per Year - based on 2600 employees MO & IL or
Cost Per Incident report, based on 50 incidents/year

7.1.1.2 Cost for Base/Minimal Service Fee

7.1.2 Case Management Services Per Year (includes 10 named User License)

7.1.3. **Total Annual recurring fees per year**

One-Time Startup Costs

7.2 Training

7.2.1 Cost per administrator course

7.2.2 Cost per case manager course

7.2.3 Cost per investigator course

TOTAL TRAINING COSTS

7.3 Employee Awareness (optional and separately priced items)

7.3.1 Web Landing Page Setup Fee

7.3.2 Email Template

7.3.3 Overview Presentation Fee

7.3.4 FAQ Fee

7.3.5 Brochure/wallet card fee

7.3.6 Program Poster Fee

7.3.7 Topical Poster Fee -4 posters

TOTAL AWARENESS COSTS

7.4 Implementation (One-Time) Fee

7.4.1 Telephonic Incident reporting set-up fee

7.4.2 Web incident reporting set-up fee

7.4.3 Case Management setup fee

7.4.4 Training setup fee

7.4.5 Employee awareness fee

7.4.6 **TOTAL IMPLEMENTATION COSTS**

TOTAL ONE-TIME COSTS (YEAR 1)

	Vendor #1				Vendor #2			Vendor #3		
	Non Bundled	Bundled - Year 1 Cost	Year 2 Cost	Year 3 Cost	Year 1 Cost	Year 2 Cost	Year 3 Cost	Year 1 Cost	Year 2 Cost	Year 3 Cost
7.1.1.1	\$ 3,495.00	\$ 2,795.00	\$ 2,795.00	\$ 2,795.00	\$ 5,910.00	\$ 5,910.00	\$ 5,910.00	\$ -	\$ -	\$ -
7.1.1.2	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 2,500.00	\$ 2,500.00	\$ 2,500.00
7.1.2	\$ 8,995.00	\$ 7,095.00	\$ 7,095.00	\$ 7,095.00	\$ -	\$ -	\$ -	\$ 1,300.00	\$ 1,300.00	\$ 1,300.00
7.1.3. Total Annual recurring fees per year	\$ 12,490.00	\$ 9,890.00	\$ 9,890.00	\$ 9,890.00	\$ 5,910.00	\$ 5,910.00	\$ 5,910.00	\$ 3,800.00	\$ 3,800.00	\$ 3,800.00
	TOTAL 3-Year Life Cycle Annual Costs \$ 29,670.00				TOTAL 3-Year Life Cycle Annual Costs \$ 17,730.00			TOTAL 3-Year Life Cycle Annual Costs \$ 11,400.00		
		# of Trainees	Total Cost		# of Trainees	Total Cost		# of Trainees	Total Cost	
7.2.1	\$ -	2	\$ -	\$ -	2	\$ -	\$ -	2	\$ -	\$ -
7.2.2	\$ -	10	\$ -	\$ -	10	\$ -	\$ -	10	\$ -	\$ -
7.2.3	\$ -	10	\$ -	\$ -	10	\$ -	\$ -	10	\$ -	\$ -
TOTAL TRAINING COSTS			\$ -			\$ -			\$ -	
		* training included			* 4 hours included for each trainee type			* 1 session included for each trainee type (Case Management includes investigator training)		
7.3.1	\$ 1,100.00	720.00		\$ -			\$ 750.00			
7.3.2	\$ 100.00	Included		\$ 1,700.00			\$ -			
7.3.3	\$ 400.00	Included		\$ -			not provided			
7.3.4	\$ 300.00	Included		N/A			\$ -			
7.3.5	\$ 1,792.00	1,792.00		\$ 540.00			\$ 1,300.00			
7.3.6	\$ 3.60	3.60		\$ 125.00			\$ 7.45			
7.3.7	\$ 14.40	14.40		\$ 3,200.00			\$ 29.80			
TOTAL AWARENESS COSTS	\$ 3,710.00	\$ 2,530.00		\$ 5,565.00			\$ 2,087.25			
7.4.1	\$ 1,500.00	2,500.00					\$ 2,500.00			
7.4.2	\$ 2,000.00	-					\$ 1,250.00			
7.4.3	\$ -	-		\$ 995.00			\$ -			
7.4.4	\$ -	-					\$ -			
7.4.5	\$ -	-					\$ -			
7.4.6 TOTAL IMPLEMENTATION COSTS	\$ 3,500.00	\$ 2,500.00		\$ 995.00			\$ 3,750.00			
TOTAL ONE-TIME COSTS (YEAR 1)	\$ 7,210.00	\$ 5,030.00		\$ 6,560.00			\$ 5,837.25			
		Year 1	Year 2	Year 3	Year 1	Year 2	Year 3	Year 1	Year 2	Year 3
TOTAL ANNUAL COSTS		\$ 14,920.00	\$ 9,890.00	\$ 9,890.00	\$ 12,470.00	\$ 5,910.00	\$ 5,910.00	\$ 9,637.25	\$ 3,800.00	\$ 3,800.00
TOTAL 3-YEAR LIFE CYCLE COSTS		\$ 34,700.00			\$ 24,290.00			\$ 17,237.25		

cost comparison to winning bid

50%

29%

Fees and Payment Schedule - All pricing is based upon the Scope of Services defined within as well as any assumptions listed in Section 8 of the solicitation document

METRO FRAUD AND ETHICS HOTLINE AND CASE MANAGEMENT SERVICES SCOPE OF WORK

Background

Bi-State Development Agency (d/b/a as “Metro”) was created in 1949 through a compact between Missouri and Illinois and ratified by the United States Congress. The compact and its enabling legislation provide broad powers that enable Metro to cross local, county, and even state boundaries in its efforts to enhance the region. It currently serves the City of St. Louis, St. Louis County, and St Clair County in Illinois, covering approximately 3,600 square miles and more than 200 municipalities and taxing districts.

Metro has the power to plan, construct, maintain, own, and operate specific public works facilities including bridges, airports, wharves, docks, grain elevators, and air, water, rail and other terminal community storage areas in addition to serving as owner and operator of the area’s public transportation system.

It is governed by a ten-member Board of Commissioners, appointed by the governors of Missouri and Illinois to alternating five-year terms without pay. Metro has no taxing authority, but it is a “quasi-public” agency authorized to issue industrial revenue bonds, collect fees, and receive funds from federal, state, local, and private sources.

Work to Be Performed

Metro wishes to retain a company to develop, implement, and provide Ethics, Conflict of Interest, Fraud, and Corruption Hotline Reporting. This service will be made available to Metro’s employees, Board of Commissioners, suppliers, and supporting contractors; and Incident Case Management services to Metro managers through telephone, Internet, and Intranet access. These services must be available 24 hours a day, 7 days a week.

Period of Performance

Services will be provided for one year, with two 1-year renewable option years.

General Requirements

1. Metro has approximately 2,600 employees in Missouri and Illinois who will contact the helpline telephonically or electronically (web form), and either file an original report or engage in a general inquiry.
2. Bid prices for each line item must be submitted on a fixed price, cost per case basis for the entire one-year period and for the two option years.

Scope of Work

The following items are included within this Scope of Work (“SOW”):

1. Incident Reporting – Reporting methods are available to all employees 24 hours per day, 365 days per year and allow for various methods for follow-up support for both named and anonymous reporters. All incident data is retained and available for a minimum of thirty-six (36) months from the date of the original report’s closure date. All incident data is translated into (if necessary), and retained in English. All calls or web incident reports will originate within the continental U.S.

1.1. Telephonic

- 1.1.1. Incident reporting calls will be placed using a toll-free number for use throughout Missouri and Illinois. If applicable, Vendor can assume ownership of an existing number for incoming calls.
- 1.1.2. Automated Welcome Message - Standard, pre-recorded message validating to the caller that they have reached the appropriate phone number.
- 1.1.3. Call Greeting – Call greeting can be customized with the specific name of Metro’s incident reporting program. Call greetings must not exceed 30 seconds.
- 1.1.4. Custom Questions – In addition to a standard proprietary incident reporting script developed by Vendor, Metro may request up to 5 additional custom questions.
- 1.1.5. Dissemination – Incident reports can be disseminated to least 10 named recipients via email, or Extensible Markup Language (XML) file by email or File Transfer Protocol (FTP). Pretty Good Privacy (PGP) encryption is desired for email transmissions.
- 1.1.6. Escalation – Escalation is based on a 3-tiered escalation criteria (e.g., High, Medium, and Low priority).
 - 1.1.6.1. For High priority incident reports (i.e., incidents requiring Metro’s immediate action due to potential threat to a person, property, or environment), Vendor must immediately escalate initial report to up to three (3) Metro contacts, by telephone only, prior to completing the report in the Vendor’s incident reporting system.
 - 1.1.6.2. For Medium priority incident reports (i.e., incidents requiring Metro’s prompt, but not immediate, action), Vendor completes the report in the Vendor’s incident reporting system and then alerts Metro’ designated recipients via email.
 - 1.1.6.3. For Low priority incident reports (i.e., incidents that do not require Metro’s immediate action), Vendor completes the report in the Vendor’s incident reporting system and then alerts Metro’ designated recipients via email.

- 1.1.7. Incident Report Response/Follow-Up Reports – The initial incident report and any follow-up reports must include an Incident Report Control Number and access code provided to the Incident Reporter during his/her initial call. In addition, the Report will include a date given to the Reporter to call back for any follow-up status.

If Metro wishes to provide a follow-up response to the Reporter, Metro will need to upload the response to the Case Management Application account before the designated follow-up date. Metro' response to the Reporter may include, but need not be limited to, additional questions concerning the reported information, a statement concerning the status of the investigation of the reported information, or a request that the Reporter contact an internal Metro representative.

If the Reporter makes a follow-up call to the Incident Reporting System phone number and can provide the Report Control Number and access code, the Vendor's customer service agent will read Metro' response to the Reporter. If the Reporter provides additional information, the Vendor's customer service agent will prepare a follow-up report containing the additional information, upload the report to Metro' Case Management Application account, and email the report or a report notice to Metro' designated Report Recipient(s).

- 1.2. Facility Locations – The full addresses of Metro's facility locations will be provided to the Vendor for uploading into Vendor's incident reporting system.

- 1.3. Incident Codes – The following standard incident codes are required:

- a. Accounting/Audit Irregularities
- b. Computer Security Issues
- c. Conflicts of Interest
- d. Metro Credit Card Abuse
- e. Customer Relations
- f. Discrimination
- g. Employee Relations
- h. Facility/Physical Security Issues
- i. Falsification of Agency Records
- j. Fraud
- k. Fraudulent Insurance Claims
- l. General Harassment
- m. Improper Loans to Executives
- n. Kickbacks
- o. Policy Issues
- p. Release of Proprietary Information
- q. Retaliation of Whistleblowers
- r. Safety Issues
- s. Sanitation Issues
- t. Security Issues
- u. Sexual Harassment

- v. Substance Abuse
- w. Theft of Cash
- x. Theft of Goods/Services
- y. Theft of Time
- z. Unauthorized Discounts
- aa. Unauthorized Gifts or Gratuities
- bb. Wage/Hour Issues
- cc. Workplace Violence/Threats

If the Vendor has additional incident codes, or includes one or more incident codes as part of another incident code name, the Vendor must list them in their response.

- 1.3.1. Incident Code Definitions – Text describing each Incident Code will default to those provided by the Vendor but can be customized for Metro-specific needs.
- 1.4. Incident Report Web Form – Vendor must provide standard employee-facing, web-based method allowing Metro employees, suppliers, and supporting contractors to enter incident reports and responses to certain critical questions in order to capture and centralize all reported incidents. Access to must be provided through Metro' Internet and Intranet web sites.
 - 1.4.1. Branding – Vendor will upload personalized logo provided by Metro.
 - 1.4.2. Incident Codes – See section [1.3](#) above
 - 1.4.3. Custom Questions – See section [1.1.4](#) above.
 - 1.4.4. File Attachments – Supporting documentation in the form of electronic files can be attached to a reported incident. No more than 10 files can be attached to a single incident report and combined size of attached files cannot exceed 10 MB. No single attached file should exceed 3 MB.
- 1.5. Incident Report Response/Follow-Up Web Form – Vendor must provide standard Web-based access allowing Metro managers to enter responses to certain critical questions in order to capture and centralize all reported issues.
 - 1.5.1. Branding – Vendor will upload personalized logo provided by Metro.
 - 1.5.2. Incident Codes – See section [1.3](#) above
 - 1.5.3. Custom Questions – See section [1.1.4](#) above.
 - 1.5.4. File Attachments – Supporting documentation in the form of electronic files can be attached to a reported incident. No more than 10 files can be attached to a single incident report and combined size of attached files cannot exceed 10 MB. No single attached file should exceed 3 MB.
- 1.6. Incident Reporting (Vendors are allowed to fulfill these requirements separately under a separate Case Management services section).

1.6.1. Activity Detail Report – Distributed monthly via email to Metro-designated recipients, this report contains the following fields for each individual event within the most recently completed month:

- Location
- Report Number
- Date of Incident
- Incident Status
- Issue Type
- City
- State
- Previously Reported to Management (Yes/No)
- Incident Summary

1.6.2. Summary Report – Distributed monthly via email to Metro-designated recipients, this report contains monthly and year-to-date summaries of:

1.6.2.1. Incident Report Activity

- Anonymous vs. non-anonymous incidents
- Escalated incidents
- Incidents previously reported to management reports
- Incident Status

1.6.2.2. Call Activity

- Total calls
- Original incident reports
- Caller callbacks
- Client follow-up

1.6.2.3. Issue Type Summary

- Call number
- Percentage by Incident Code
- Incident Status

1.6.3. Standard Report Library - Metro users have the ability to select Vendor-provided standard reports, apply filters to those reports, and produce reports for print or electronic distribution.

1.6.4. Report Wizard – Metro users have the ability to create, save, and share custom reports to display specific details, summary overviews, or graphical representations.

2. Case Management – The goals for Case Management are to:

- Ensure that every incident, regardless of how it is reported, is centrally managed and everyone involved knows what needs to be done, and is resolved in a timely manner.

- Provide a comprehensive view of all incident activity across Metro, offering an audit trail of every incident from allegation to investigation to resolution, allowing instant analysis and the ability to address critical issues quickly. All case management data is retained and available for a minimum of thirty-six (36) months from the case closed date.
- 2.1. All case information is to be displayed, retained, and reported on in English.
 - 2.2. Incident Data – The Case Management system will automatically populate with all incident data from all available network incident-reporting mechanisms/services purchased by Metro.
 - 2.3. Initial User Setup – Vendor will create initial user profiles, standard roles (Administrator, Case Manager, and Investigator) and at least three (3) customized work groups and workflows.
 - 2.4. Location Hierarchy – Vendor will configure system with the Metro’s facility locations and organizational hierarchy.
 - 2.5. Standard Portal and Dashboard Implementation – Vendor must provide Metro users with a gateway to the Case Management system.
 - 2.6. Branding – Vendor will upload personalized logo provided by Metro.
 - 2.7. Workflows – Case Management will utilize the Vendor’s own defined standard best practice workflows for the incidents types identified in section [1.3](#) above.
 - 2.8. Business rules – Case Management will be configured with the following Vendor-defined standard best practice business rules for :
 - 2.8.1. Notification upon Case Assignment (no conditionality applied).
 - 2.8.2. Notification upon Response/Follow-up Received (no conditionality applied).
 - 2.9. System Configuration – Vendor will work with Metro to configure the following:
 - Case Class
 - Status Types
 - Priority Types
 - Risk Types
 - Outcome Types
 - Disposition Types
 - File Categories
 - Notes Categories
 - Involved Party Types Categories.
 - 2.10. Reporting and Analytics
 - 2.10.1. User Permissions – Metro must have the ability to grant access to Reporting and Analytics to any user that has a login to Case Management.

- 2.10.2. Standard Reports – Reporting and Analytics will be configured with the following Vendor-defined standard best practice reports that cover:
 - 2.10.2.1. Activity by Location
 - 2.10.2.2. Activity by Hierarchy
 - 2.10.2.3. Case Status Count
 - 2.10.2.4. Cases Closed in Last X Days
 - 2.10.2.5. Workload by Assignee
 - 2.10.2.6. Cases due in Next X Days
- 2.10.3. Standard Dashboard Widgets – Reporting and Analytics will be configured with Vendor-defined standard best practice dashboard web-based widgets that cover:
 - 2.10.3.1. Activity by Hierarchy
 - 2.10.3.2. Case Status Count
 - 2.10.3.3. Cases Closed in Last X Days
 - 2.10.3.4. Workload by Assignee
 - 2.10.3.5. Cases Due in Next X Days
- 2.10.4. Metro requires the ability to create custom reports utilizing the Vendor's standard templates.
- 2.10.5. Metro desires to have the ability to create custom dashboard widgets from their custom reports.
- 2.10.6. Customizable Default Dashboard Roles – Vendor will work with Metro to determine the naming convention for up to 5 default dashboard roles to be used in Reporting and Analytics. (Building of the default dashboards will be done by Metro staff assigned to those roles.)
- 3. System Administration – Two (2) Metro Administrators will be identified for adding or deleting Administrator, Case Manager, and Investigator users, resetting passwords, and running ad-hoc reports.
- 4. Employee Communication and Awareness (**all items are optional and separately priced**) - Vendor will prepare ready-made electronic versions of print media to educate and promote ethics hotline and ethics program to Metro employees. Metro will utilize Vendor's standard materials with only minimal customization. Since Metro has its own in-house print center, Vendor will authorize reproduction and provide originals in Adobe PDF format. Metro will provide its logo in color in the Vendor's desired electronic format as much as possible.
 - 4.1. Web Landing Page – Themed Web page displaying program message, telephonic Incident reporting number(s), and Uniform Resource Locator (URL) for Incident Report Web Form (see section [1.4](#) above). Configurable components include Metro' specific list of Reportable Activities.

- 4.2. Employee Email Templates:
 - 4.2.1. Employee Template – Vendor will provide a draft message to be used in a Metro-administered email campaign notifying employees of program.
 - 4.2.2. Manager Template – Vendor will provide a draft message to be used in a Metro-administered email campaign encouraging managers to promote program among employees.
- 4.3. Overview Presentation – Vendor will provide their standard PowerPoint presentation template to be used in a Metro-administered incident reporting awareness campaign.
- 4.4. FAQs – themed file containing questions frequently asked about incident reporting programs. .
- 4.5. Brochure with Wallet Card – Themed tri-fold brochure (8.5” by 11”) with removable wallet card displaying program message, telephonic Incident reporting number(s), and URL for Incident Report Web Form (see section [1.4](#) above). Configurable components include Metro-specific list of Reportable Activities.
- 4.6. Program Poster – Vendor will provide a themed program poster (11” wide by 17” tall) displaying incident reporting program message, telephonic Incident reporting number(s), and URL for Incident Report Web Form (see section [1.4](#) above).
- 4.7. Other Topical Posters – Metro may select four (4) posters (11” wide by 17” tall) for display from Vendor’s library of Vendor-developed posters.
- 4.8. Introductory Letter and Envelope – Vendor will provide a single-page letter for promoting the incident-reporting program to Metro employees and contractors. Configurable components include:
 - 4.8.1. Metro Letterhead – Metro will provide letterhead in monochrome and color in the vendor’s desired electronic format as much as possible.
 - 4.8.2. Signature – Metro-provided image of signature from Metro program promoter.
 - 4.8.3. Letter Content – Vendor will supply sample messaging that can be used by Metro or Metro can provide corporate messaging to be used.
 - 4.8.4. Envelopes – Metro will provide its own #10 size pre-printed envelopes for this mailing.
5. Training – Vendor will provide role-based Incident Reporting and Case Management training to Metro’ Administrators (2), Case Managers (up to 10), and Investigators (up to 10). The Vendor will host all courses through webinars, or the Vendor’s own in-line training system or website.

6. Implementation Methodology - Once this SOW is awarded with a subsequent contract award, Vendor will follow Vendor's standard implementation approach to ensure the timely delivery of a solution that meets or exceeds all defined Metro' requirements. Based on product selection and complexity of implementation, these steps may be conducted by email, phone, or in-person meetings. Steps of this approach will include:

- 6.1. Establishment of Vendor and Metro project teams.
- 6.2. Implementation kick-off to outline the implementation process, develop a project schedule, and set the tone for the project.
- 6.3. Assessing and defining Metro' needs.
- 6.4. Making recommendations based on Vendor's best business practice experience (as needed).
- 6.5. Defining required system configuration.
- 6.6. System testing and user acceptance testing.
- 6.7. Administrator and end-user training (as needed).
- 6.8. Metro rollout and post-implementation validation.
- 6.9. Post rollout support for up to 30 days after go live.

7. Fees and Payment Schedule - All Pricing is based upon the Scope of Services defined above as well as any assumptions listed in section 8 below.

7.1. Annual Fees

7.1.1. Incident reporting Services: Fees can be quoted as:

7.1.1.1. \$_____ per year, based on 2,600 employees in Missouri and Illinois; or

\$_____ per incident report, based on 50 incidents/year

7.1.1.2. \$_____ for base/minimal Service fee

7.1.2. Case Management Services: \$_____ per year, which includes 10 named User licenses.

7.1.3. Total Annual Recurring Fees: \$_____ per year.

7.2. Training:

7.2.1. \$_____ per Administrator course

7.2.2. \$_____ per Case Manager course

7.2.3. \$_____ per Investigator course

7.3. Employee Awareness (optional)

- 7.3.1. Web Landing Page Set-up Fee: \$_____
- 7.3.2. Email Template Fee: \$_____
- 7.3.3. Overview Presentation Fee: \$_____
- 7.3.4. FAQ Fee: \$_____
- 7.3.5. Brochure/wallet card Fee: \$_____
- 7.3.6. Program Poster Fee: \$_____
- 7.3.7. Topical Poster Fee: \$_____ per poster; \$_____ for 4 posters

7.4. Implementation (One-Time) Fees

- 7.4.1. Telephonic Incident reporting Set-up Fee: \$_____
- 7.4.2. Web Incident reporting Set-up Fee: \$_____
- 7.4.3. Case Management Set-up Fee: \$_____
- 7.4.4. Training Set-up Fee: \$_____
- 7.4.5. Employee Awareness Fee: \$_____
- 7.4.6. Total One-Time Set-up Fees: \$_____

7.5. Implementation Fees described herein are subject to change based on the Change Management process described in section 9 below.

7.6. Payment Schedule – Implementation fees will be billed upon completion of all required implementation tasks, the specified services have become operational, and Metro has confirmed final user acceptance. Annual and Additional Fees are billed annually in advance of providing services. If incident report volume exceeds transactional limits, additional per report fees will be invoiced monthly. Metro shall pay invoiced amounts within thirty (30) days after receipt of invoice.

8. Definitions/Assumptions

- 8.1. Telephonic Report – A telephone call that alleges a violation of Metro’ standards of conduct.
- 8.2. Web Report – A report that is entered via the web and does not require a telephonic interview.
- 8.3. General Inquiry – A call that does not allege a violation of Metro’ standards of conduct, such as benefits questions, payroll questions or any other matter for which Metro requires Vendor to refer the person making the call to a Metro department.

8.4. All business conversations and training will be conducted in English unless otherwise agreed to by both parties.

9. Change Management

SOW Change Request Process. Scope control is a priority during the term of this SOW. A Change Request ("CR") is defined as a written agreement between the Parties for additions, modifications, or deletions to this SOW. The following provides a detailed procedure to follow if a change to this SOW is desired. The Parties will handle all proposed changes through the following process:

- 9.1. Metro and/or Vendor will identify a desired change and give the other Party a written notice thereof ("Notice of Proposed Change").
- 9.2. Vendor will determine the impact of the desired change on Project scope, schedule, and/or budget, and will provide Metro with a written statement of such impact ("Statement of Impact") concurrently with any Notice of Proposed Change given to Metro or within a commercially reasonable time after either Party documents a Notice of Proposed Change.
- 9.3. Metro will review the Statement of Impact and may request additional information. Vendor may specify commercially reasonable fees to be charged, if any, to reimburse Vendor for expenses to be incurred in providing such additional information with respect to any Notice of Proposed Change initiated by Metro.
- 9.4. If both Parties desire to implement the proposed change, the Parties will jointly develop a CR describing the proposed change and the rationale for such change. If the CR is acceptable to both Parties, the Metro and Vendor will each sign and deliver the CR to the other, which will then constitute the Parties' binding agreement to the proposed change and any associated fees provided for therein.
- 9.5. Vendor will invoice Metro for any additional charges provided for in the CR.

ATTACHMENT 1 – Standard Ethic Hotline Allegations Definition List

Allegation	Definition
Discrimination	Statements or actions based on age, race, color, national origin, sexual orientation, gender, disability, or religion that are the basis for employment, promotion, or compensation decisions.
Harassment – Sexual	Statements or actions expressing unwelcome sexual advances, requests for sexual favors, unsolicited physical contact or propositions, unwelcome flirtations, or offensive verbal or visual expressions or physical conduct of a sexual nature.
Harassment – Workplace	Persistent statements, conduct, or actions that are uninvited, degrading, offensive, humiliating, or intimidating and create an unpleasant or hostile environment.
Retaliation or Retribution	Statements or actions discharging, demoting, suspending, threatening, harassing or discriminating against an employee because of any lawful act taken by such employee in connection with reporting a violation of law or policy, filing a complaint, or assisting with an investigation or proceeding.
Conflict of Interest – Personal	Any personal interest, any business or professional activity or relationship, prior or current employment, or any obligation that may interfere with the ability to objectively perform job duties and responsibilities or impair independence and objectivity.
Inappropriate Behavior	Statements or actions that are not harassing in nature, but are believed to be unsuitable for the workplace.
Unfair Employment Practices	Employment decisions, practices or disciplinary actions that are believed to be unfair regardless of whether they are the result of job performance, changes in business needs or other business related decisions.
Environment, Health and Safety	Conduct, actions, policies or practices that either violate local, provincial or federal environmental, health or safety laws or regulations or may cause or result in potentially hazardous conditions that impact the environment or the health or safety of employees, customers or others.
Substance Abuse	The unlawful use, possession, sale, conveyance, distribution, concealment, transportation or manufacture of illegal drugs, intoxicants, controlled substances or drug paraphernalia in the workplace or while conducting business.
Threats and Physical Violence	Statements or actions that threaten acts of violence or the presence of weapons, firearms, ammunition, explosives or incendiary devices in the workplace, on work premises or in work vehicles
Accounting and Auditing Practices	Statements or actions that violate or conflict with either internal policies, procedures, or practices or government regulations related to the detailed reporting of the financial state or transactions of an organization or the examination, verification, or correction of its financial accounts.
Conflict of Interest – Financial	Any financial interest, any business or professional activity, prior or current employment, or any obligation that may interfere with the ability to objectively perform job duties and responsibilities or impair independence and objectivity.
Gifts, Bribes and Kickbacks	Payments, payments in kind, gifts, bribes, extensions of credit or benefits extended to or received by customers, employees, suppliers, vendors, competitors, directors, officers, auditors, government employees, government officials or agencies, or other parties that are unlawful, improper, or designed to influence business decisions or political processes.
Trading on Inside Information	The purchase, sale of stock, or other securities based on non-public and material information obtained during the course of employment or providing such information to another person who purchases, sells stock, or other securities based upon that information.
Customer Relations	Statements or actions that are negatively impacting or interfering with customers, customer relationships, or customer agreements.
Disclosure of Confidential Information	The unauthorized or illegal disclosure, copying, duplication, misuse or release of confidential or personal data including but not limited to employment, financial, medical and health, customer lists, contracts, business plans, personnel records or other property marked or generally regarded as confidential or trade secrets.

Allegation	Definition
Misuse of Resources	The improper, unauthorized, or unlicensed use of property or resources for non-business related reasons or purposes including improper use of systems and timekeeping.
Theft	The unauthorized removal or taking of supplies, equipment, furniture, fixtures, products, cash, merchandise, or other tangible property.
Guidance Request	Request for guidance, interpretation, or other information regarding matters of law, regulations, or policies.
Other	Statements actions or policies that concern the caller but are not currently resulting in harm, injury, or corporate liability and cannot be included in any other category.
Antitrust or Fair Trading	Discussions or agreements with competitors about prices or credit terms, submission of bids or offers, allocation of markets or customers, restrictions on production, distribution or boycotts of suppliers or customers that would result in monopolization or anticompetitive markets.
Espionage or Sabotage	Actions that result in the gathering, receipt or acceptance of non-public confidential information or trade secrets about competitors to gain a competitive advantage or the deliberate destruction, disruption or damage to a competitor's equipment or property for competitive advantage or gain.
Falsification or Destruction of Information	Statements or actions that encourage or result in unlawful, untimely, false, or intentional misrepresentation, concealment or destruction of information in order to deceive or mislead.
Quality Control	Complaints about product or service quality or effectiveness; allegations of product tampering; violation of policies and practices for manufacturing controls; allegations of non-compliance with product standards or service delivery.

Compliance and Fraud Helpline RFP Scores

Grading Criteria

0	1	2	3	4	5
Not meet requirement	partially meets requirement	Meets Requirement	Exceeds Requirement		

Requirement	Technical Evaluator #1			Technical Evaluator #2		
	Vendor Scores			Vendor Scores		
Incident Reporting	Vendor #1	Vendor #2	Vendor #3	Vendor #1	Vendor #2	Vendor #3
1.0						
1.1.1						
1.1.2						
1.1.3						
1.1.4						
1.1.5						
1.1.6.0 / 1.1.6.1						
1.1.6.2						
1.1.6.3						
1.1.7						
1.2.0						
1.3.0						
1.3.1						
1.4.0 /1.4.1						
1.4.2						
1.4.3						
1.4.4						
1.5.0 / 1.5.1						
1.5.2						
1.5.3						
1.5.4						
1.6.0 / 1.6.1						
1.6.2.0 / 1.6.2.1						
1.6.2.2						
1.6.2.3						
1.6.3						
1.6.4						
Total	0	0	0	0	0	0
Case Management						
2.0						
2.1.0						
2.2.0						
2.3.0						
2.4.0						
2.5.0						
2.6.0						
2.7.0						
2.8.0						
2.9.0						
Total	0	0	0	0	0	0
Reporting & Analytics						
2.10.0 / 2.10.1						
2.10.2						
2.10.3						
2.10.4						
2.10.5						
2.10.6						
Total	0	0	0	0	0	0

Compliance and Fraud Helpline RFP Scores

Grading Criteria

0	1	2	3	4	5
Not meet requirement	partially meets requirement	Meets Requirement	Exceeds Requirement		

Requirement	Technical Evaluator #1			Technical Evaluator #2		
	Vendor Scores			Vendor Scores		
	Vendor #1	Vendor #2	Vendor #3	Vendor #1	Vendor #2	Vendor #3
Incident Reporting						
System Administration						
3.0	0	0	0	0	0	0
Employee Communication						
4.0						
4.1.0						
4.2.0 / 4.2.1						
4.2.2						
4.3.0						
4.4.0						
4.5.0						
4.6.0						
4.7.0						
4.8.0						
Total	0	0	0	0	0	0
Training						
5.0						
Implementation						
6.0.0 / 6.1.0						
6.2.0						
6.3.0						
6.4.0						
6.5.0						
6.6.0						
6.7.0						
6.8.0						
6.9.0						
Total	0	0	0	0	0	0
Change Management						
9.0	0	0	0	0	0	0
GRAND TOTAL	0	0	0	0	0	0
GRAND TOTAL without optional Employee Communication	0	0	0	0	0	0

Technical Requirements – COMPLIANCE AND FRAUD HELPLINE AND CASE MANAGEMENT SERVICES

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
1.	1. Incident Reporting – Reporting methods are available to all employees 24 hours per day, 365 days per year and allow for various methods for follow-up support for both named and anonymous reporters. All incident data is retained and available for a minimum of thirty-six (36) months from the date of the original report’s closure date. All incident data is translated into (if necessary), and retained in English. All calls or web incident reports will originate within the continental U.S.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
2.	1.1. Telephonic 1.1.1. Incident reporting calls will be placed using a toll-free number for use throughout Missouri and Illinois. If applicable, Vendor can assume ownership of an existing number for incoming calls.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
3.	1.1.2. Automated Welcome Message - Standard, pre-recorded message validating to the caller that they have reached the appropriate phone number.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
4.	1.1.3. Call Greeting – Call greeting can be customized with the specific name of Client’s incident reporting program. Call greetings must not exceed 30 seconds.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
5.	1.1.4. Custom Questions – In addition to a standard proprietary incident reporting script developed by Vendor, Client may request up to 5 additional custom questions.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
6.	1.1.5. Dissemination – Incident reports can be disseminated to least 10 named recipients via email, or Extensible Markup Language (XML) file by email or File Transfer Protocol (FTP). Pretty Good Privacy (PGP) encryption is desired for email transmissions.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
7.	<p>1.1.6. Escalation – Escalation is based on a 3-tiered escalation criteria (e.g., High, Medium, and Low priority).</p> <p>1.1.6.1. For High priority incident reports (i.e., incidents requiring Client’s immediate action due to potential threat to a person, property, or environment), Vendor must immediately escalate initial report to up to three (3) Client contacts, by telephone on</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
8.	<p>1.1.6.2. For Medium priority incident reports (i.e., incidents requiring Client’s prompt, but not immediate, action), Vendor completes the report in the Vendor’s incident reporting system and then alerts Client’ designated recipients via email.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
9.	<p>1.1.6.3. For Low priority incident reports (i.e., incidents that do not require Client’s immediate action), Vendor completes the report in the Vendor’s incident reporting system and then alerts Client’ designated recipients via email.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
10.	<p>1.1.7. Incident Report Response/Follow-Up Reports – The initial incident report and any follow-up reports must include an Incident Report Control Number and access code provided to the Incident Reporter during his/her initial call. In addition, the Report will include a date given to the Reporter to call back for any follow-up status. If Client wishes to provide a follow-up response to the Reporter, Client will need to upload the response to the Case Management Application account before the designated follow-up date. Client’ response to the Reporter may include, but need not be limited to, additional questions concerning the reported information, a statement concerning the status of the investigation of the reported information, or a request that the Reporter contact an internal Client representative.</p> <p>If the Reporter makes a follow-up call to the Incident Reporting System phone number and can provide the Report Control Number and access code, the Vendor’s customer service agent will read Client’ response to the Reporter. If the Reporter provides additional information, the Vendor’s customer service agent will prepare a follow-up report containing the additional information, upload the report to Client’ Case Management Application account, and email the report or a report notice to Client’ designated Report Recipient(s).</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
11.	<p>1.2. Facility Locations – The full addresses of Client’s facility locations will be provided to the Vendor for uploading into Vendor’s incident reporting system.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
12.	<p>1.3. Incident Codes – The following standard incident codes are required:</p> <ul style="list-style-type: none"> a. Accounting/Audit Irregularities b. Computer Security Issues c. Conflicts of Interest d. Client Credit Card Abuse e. Customer Relations f. Discrimination g. Employee Relations h. Facility/Physical Security Issues i. Falsification of Agency Records j. Fraud k. Fraudulent Insurance Claims l. General Harassment m. Improper Loans to Executives n. Kickbacks o. Policy Issues p. Release of Proprietary Information q. Retaliation of Whistleblowers r. Safety Issues s. Sanitation Issues t. Security Issues u. Sexual Harassment v. Substance Abuse w. Theft of Cash x. Theft of Goods/Services y. Theft of Time z. Unauthorized Discounts aa. Unauthorized Gifts or Gratuities bb. Wage/Hour Issues cc. Workplace Violence/Threats <p>If the Vendor has additional incident codes, or includes one or more incident codes as part of another incident code name, the Vendor must list them in their response.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
13.	1.3.1. Incident Code Definitions – Text describing each Incident Code will default to those provided by the Vendor but can be customized for Client-specific needs.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
14.	<p>1.4. Incident Report Web Form – Vendor must provide standard employee-facing, web-based method allowing Client employees, suppliers, and supporting contractors to enter incident reports and responses to certain critical questions in order to capture and centralize all reported incidents. Access to must be provided through Client' Internet and Intranet web sites.</p> <p>1.4.1. Branding – Vendor will upload personalized logo provided by Client.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
15.	1.4.2. Incident Codes – See section 1.3 above	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
16.	1.4.3. Custom Questions – See section 1.1.4 above.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
17.	1.4.4. File Attachments – Supporting documentation in the form of electronic files can be attached to a reported incident. No more than 10 files can be attached to a single incident report and combined size of attached files cannot exceed 10 MB. No single attached file should exceed 3 MB.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
18.	<p>1.5. Incident Report Response/Follow-Up Web Form – Vendor must provide standard Web-based access allowing Client managers to enter responses to certain critical questions in order to capture and centralize all reported issues.</p> <p>1.5.1. Branding – Vendor will upload personalized logo provided by Client.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
19.	1.5.2. Incident Codes – See section 1.3 above	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
20.	1.5.3. Custom Questions – See section 1.1.4 above.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
21.	1.5.4. File Attachments – Supporting documentation in the form of electronic files can be attached to a reported incident. No more than 10 files can be attached to a single incident report and combined size of attached files cannot exceed 10 MB. No single attached file should exceed 3 MB.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
22.	<p>1.6. Incident Reporting (Vendors are allowed to fulfill these requirements separately under a separate Case Management services section).</p> <p>1.6.1. Activity Detail Report – Distributed monthly via email to Client-designated recipients, this report contains the following fields for each individual event within the most recently completed month:</p> <ul style="list-style-type: none"> • Location • Report Number • Date of Incident • Incident Status • Issue Type • City • State • Previously Reported to Management (Yes/No) • Incident Summary 	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
23.	1.6.2. Summary Report – Distributed monthly via email to Client-designated recipients, this report contains monthly and year-to-date summaries of: 1.6.2.1. Incident Report Activity <ul style="list-style-type: none"> o Anonymous vs. non-anonymous incidents o Escalated incidents o Incidents previously reported to management reports o Incident Status 	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
24.	1.6.2.2. Call Activity <ul style="list-style-type: none"> o Total calls o Original incident reports o Caller callbacks o Client follow-up 	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
25.	1.6.2.3. Issue Type Summary <ul style="list-style-type: none"> o Call number o Percentage by Incident Code o Incident Status 	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
26.	1.6.3. Standard Report Library - Client users have the ability to select Vendor-provided standard reports, apply filters to those reports, and produce reports for print or electronic distribution.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
27.	1.6.4. Report Wizard – Client users have the ability to create, save, and share custom reports to display specific details, summary overviews, or graphical representations.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
28.	2. Case Management – The goals for Case Management are to: <ul style="list-style-type: none"> • Ensure that every incident, regardless of how it is reported, is centrally managed and everyone involved knows what needs to be done, and is resolved in a timely manner. • Provide a comprehensive view of all incident activity across Client, offering an audit trail of every incident from allegation to investigation to resolution, allowing instant analysis and the ability to address critical issues quickly. All case management data is retained and available for a minimum of thirty-six (36) months from the case closed date. 							
29.	2.1. All case information is to be displayed, retained, and reported on in English.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
30.	2.2. Incident Data – The Case Management system will automatically populate with all incident data from all available network incident-reporting mechanisms/services purchased by Client.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
31.	2.3. Initial User Setup – Vendor will create initial user profiles, standard roles (Administrator, Case Manager, and Investigator) and at least three (3) customized work groups and workflows.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
32.	2.4. Location Hierarchy – Vendor will configure system with the Client’s facility locations and organizational hierarchy.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
33.	2.5. Standard Portal and Dashboard Implementation – Vendor must provide Client users with a gateway to the Case Management system.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
34.	2.6. Branding – Vendor will upload personalized logo provided by Client.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
35.	2.7. Workflows – Case Management will utilize the Vendor’s own defined standard best practice workflows for the incidents types identified in section 1.3 above.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
36.	2.8. Business rules – Case Management will be configured with the following Vendor-defined standard best practice business rules for : 2.8.1. Notification upon Case Assignment (no conditionality applied). 2.8.2. Notification upon Response/Follow-up Received (no conditionality applied).	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
37.	2.9. System Configuration – Vendor will work with Client to configure the following: <ul style="list-style-type: none"> • Case Class • Status Types • Priority Types • Risk Types • Outcome Types • Disposition Types • File Categories • Notes Categories • Involved Party Types Categories. 	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
38.	2.10. Reporting and Analytics 2.10.1. User Permissions – Client must have the ability to grant access to Reporting and Analytics to any user that has a login to Case Management.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
39.	2.10.2. Standard Reports – Reporting and Analytics will be configured with the following Vendor-defined standard best practice reports that cover: 2.10.2.1. Activity by Location 2.10.2.2. Activity by Hierarchy 2.10.2.3. Case Status Count 2.10.2.4. Cases Closed in Last X Days 2.10.2.5. Workload by Assignee 2.10.2.6. Cases due in Next X Days	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
40.	2.10.3. Standard Dashboard Widgets – Reporting and Analytics will be configured with Vendor-defined standard best practice dashboard web-based widgets that cover: 2.10.3.1. Activity by Hierarchy 2.10.3.2. Case Status Count 2.10.3.3. Cases Closed in Last X Days 2.10.3.4. Workload by Assignee 2.10.3.5. Cases Due in Next X Days	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
41.	2.10.4. Client requires the ability to create custom reports utilizing the Vendor’s standard templates.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
42.	2.10.5. Client desires to have the ability to create custom dashboard widgets from their custom reports.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
43.	2.10.6. Customizable Default Dashboard Roles – Vendor will work with Client to determine the naming convention for up to 5 default dashboard roles to be used in Reporting and Analytics. (Building of the default dashboards will be done by Client staff assigned to those roles.)	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
44.	3. System Administration – Two (2) Client Administrators will be identified for adding or deleting Administrator, Case Manager, and Investigator users, resetting passwords, and running ad-hoc reports.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
45.	<p>4. Employee Communication and Awareness (all items are optional and separately priced) –</p> <p>Vendor will prepare ready-made electronic versions of print media to educate and promote ethics hotline and ethics program to Client employees. Client will utilize Vendor’s standard materials with only minimal customization. Since Client has its own in-house print center, Vendor will authorize reproduction and provide originals in Adobe PDF format. Client will provide its logo in color in the Vendor’s desired electronic format as much as possible.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
46.	<p>4.1. Web Landing Page – Themed Web page displaying program message, telephonic Incident reporting number(s), and Uniform Resource Locator (URL) for Incident Report Web Form (see section 1.4 above). Configurable components include Client’ specific list of Reportable Activities.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
47.	<p>4.2. Employee Email Templates: 4.2.1. Employee Template – Vendor will provide a draft message to be used in a Client-administered email campaign notifying employees of program.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
48.	<p>4.2.2. Manager Template – Vendor will provide a draft message to be used in a Client-administered email campaign encouraging managers to promote program among employees.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
49.	<p>4.3. Overview Presentation – Vendor will provide their standard PowerPoint presentation template to be used in a Client-administered incident reporting awareness campaign.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
50.	<p>4.4. FAQs – themed file containing questions frequently asked about incident reporting programs.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
51.	4.5. Brochure with Wallet Card – Themed tri-fold brochure (8.5” by 11”) with removable wallet card displaying program message, telephonic Incident reporting number(s), and URL for Incident Report Web Form (see section 1.4 above). Configurable components include Client-specific list of Reportable Activities.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
52.	4.6. Program Poster – Vendor will provide a themed program poster (11” wide by 17” tall) displaying incident reporting program message, telephonic Incident reporting number(s), and URL for Incident Report Web Form (see section 1.4 above).	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
53.	4.7. Other Topical Posters – Client may select four (4) posters (11” wide by 17” tall) for display from Vendor’s library of Vendor-developed posters.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
54.	4.8. Introductory Letter and Envelope – Vendor will provide a single-page letter for promoting the incident-reporting program to Client employees and contractors. Configurable components include: 4.8.1. Client Letterhead – Client will provide letterhead in monochrome and color in the vendor’s desired electronic format as much as possible. 4.8.2. Signature – Client-provided image of signature from Client program promoter. 4.8.3. Letter Content – Vendor will supply sample messaging that can be used by Client or Client can provide corporate messaging to be used. 4.8.4. Envelopes – Client will provide its own #10 size pre-printed envelopes for this mailing.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
55.	5. Training – Vendor will provide role-based Incident Reporting and Case Management training to Client’ Administrators (2), Case Managers (up to 10), and Investigators (up to 10). The Vendor will host all courses through webinars, or the Vendor’s own in-line training system or website.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
56.	6. Implementation Methodology - Once this SOW is awarded with a subsequent contract award, Vendor will follow Vendor's standard implementation approach to ensure the timely delivery of a solution that meets or exceeds all defined Client' requirements. Based on product selection and complexity of implementation, these steps may be conducted by email, phone, or in-person meetings. Steps of this approach will include: 6.1. Establishment of Vendor and Client project teams.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
57.	6.2. Implementation kick-off to outline the implementation process, develop a project schedule, and set the tone for the project.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
58.	6.3. Assessing and defining Client' needs.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
59.	6.4. Making recommendations based on Vendor's best business practice experience (as needed).	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
60.	6.5. Defining required system configuration.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
61.	6.6. System testing and user acceptance testing.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
62.	6.7. Administrator and end-user training (as needed).	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
63.	6.8. Client rollout and post-implementation validation.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		

No.	Requirement	Vendor #1 Response	Points (1-5 Scale)	Vendor #2 Response	Points (1-5 Scale)	Vendor #3 Response	Points (1-5 Scale)	Notes
64.	6.9. Post rollout support for up to 30 days after go live.	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		
65.	Note: Section 7 contains Fees Section 8 contains terms and definitions							
66.	<p>9. Change Management SOW Change Request Process. Scope control is a priority during the term of this SOW. A Change Request ("CR") is defined as a written agreement between the Parties for additions, modifications, or deletions to this SOW</p> <p>9.1. Client and/or Vendor will identify a desired change and give the other Party a written notice thereof ("Notice of Proposed Change").</p> <p>9.2. Vendor will determine the impact of the desired change on Project scope, schedule, and/or budget, and will provide Client with a written statement of such impact ("Statement of Impact") concurrently with any Notice of Proposed Change given to Client or within a commercially reasonable time after either Party documents a Notice of Proposed Change.</p> <p>9.3. Client will review the Statement of Impact and may request additional information. Vendor may specify commercially reasonable fees to be charged, if any, to reimburse Vendor for expenses to be incurred in providing such additional information with respect to any Notice of Proposed Change initiated by Client.</p> <p>9.4. If both Parties desire to implement the proposed change, the Parties will jointly develop a CR describing the proposed change and the rationale for such change. If the CR is acceptable to both Parties, the Client and Vendor will each sign and deliver the CR to the other, which will then constitute the Parties' binding agreement to the proposed change and any associated fees provided for therein.</p> <p>9.5. Vendor will invoice Client for any additional charges provided for in the CR.</p>	<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		<input type="checkbox"/> Meet <input type="checkbox"/> Does Not Meet <input type="checkbox"/> Exceed		