SCCE’s 18th Annual
Compliance & Ethics Institute

1

Session 206:
Password Techniques and Strategies to Promote a Higher Level of IT Security

Frank Ruelas,
Facility Compliance Professional
St. Joseph’s Hospital and Medical Center/Dignity Health
(francisco.ruelas@dignityhealth.org)

1

SCCE’s 18th Annual
Compliance & Ethics Institute

2

Se
Passw to
ecurity

Frank Ru
Facility C onal
St. Joseph and Medical Center/Dignity Health
(francisco.r elas@dignityhealth.org)

Lunch follows this session!

2

3

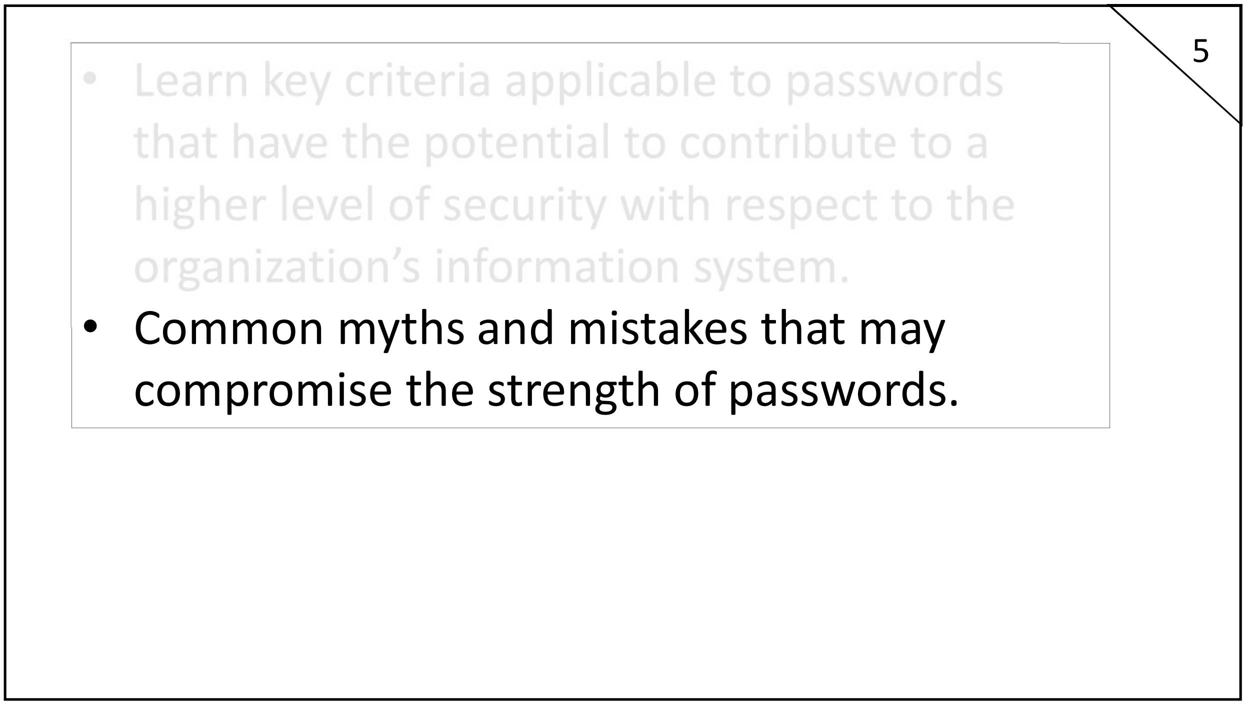
Objectives… Let’s break them down.

3

4

- Learn key criteria applicable to passwords that have the potential to contribute to a higher level of security with respect to the organization’s information system.

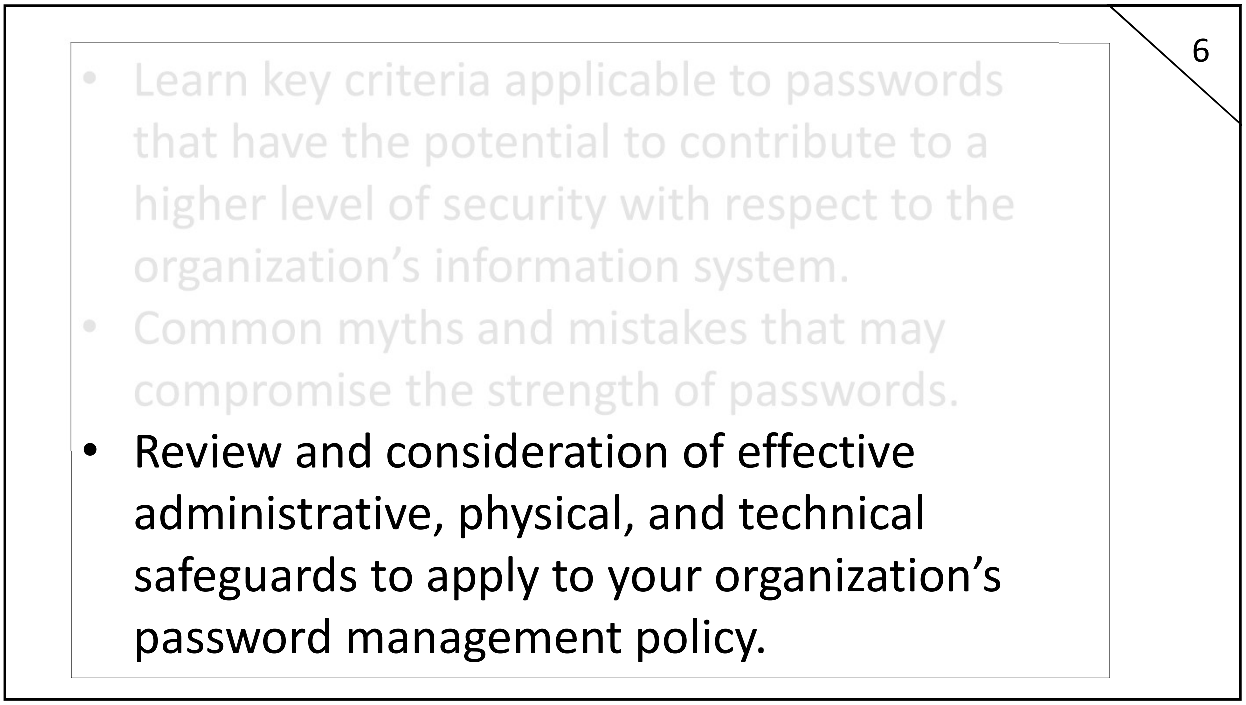
4



5

- Learn key criteria applicable to passwords that have the potential to contribute to a higher level of security with respect to the organization’s information system.
- Common myths and mistakes that may compromise the strength of passwords.

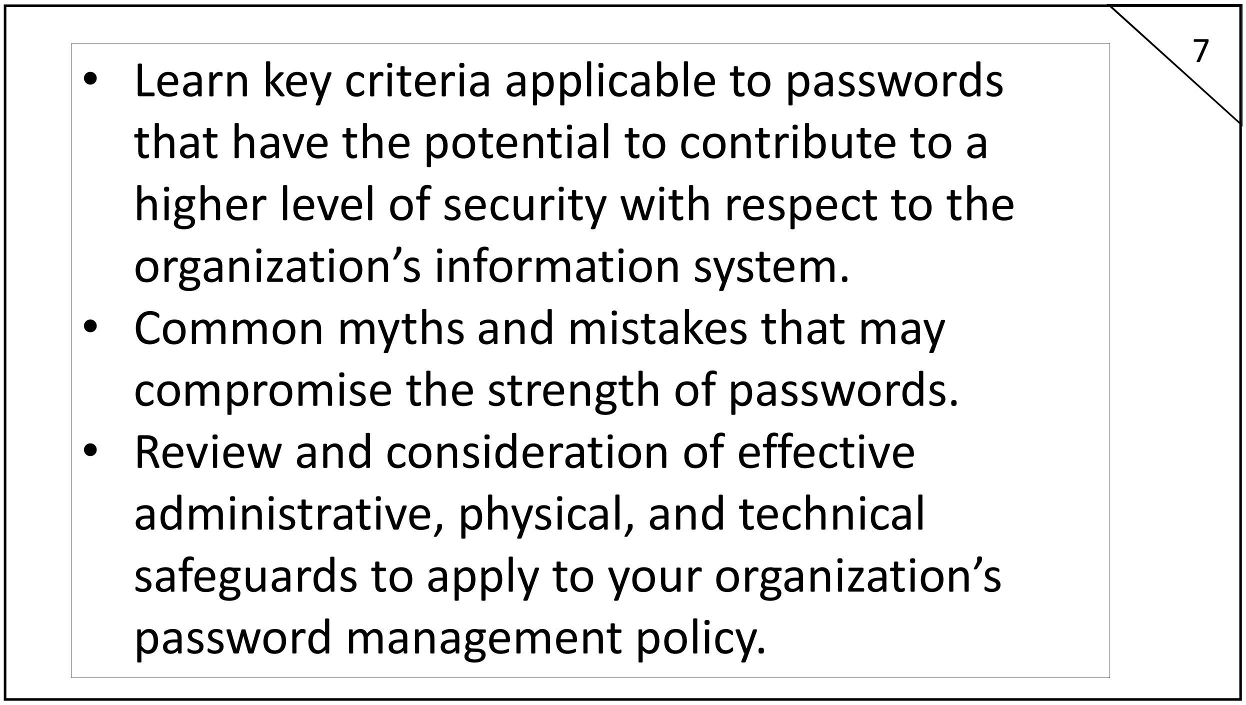
5



6

- Learn key criteria applicable to passwords that have the potential to contribute to a higher level of security with respect to the organization’s information system.
- Common myths and mistakes that may compromise the strength of passwords.
- Review and consideration of effective administrative, physical, and technical safeguards to apply to your organization’s password management policy.

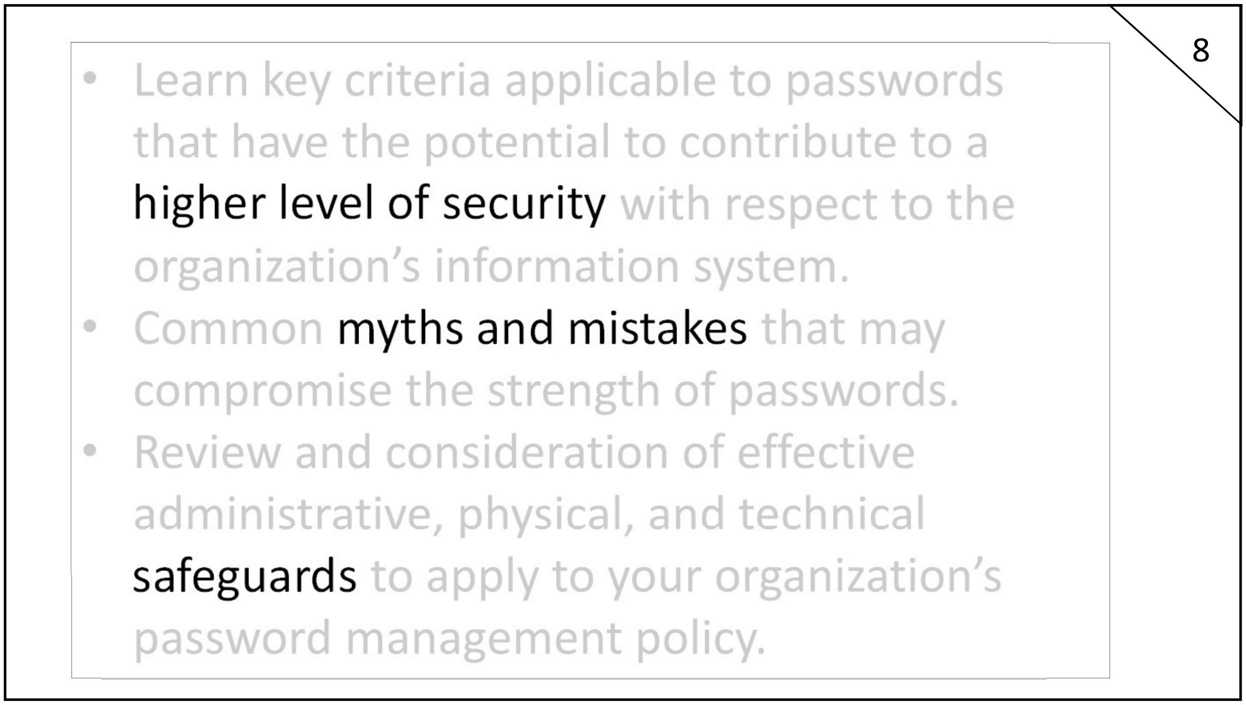
6



7

- Learn key criteria applicable to passwords that have the potential to contribute to a higher level of security with respect to the organization’s information system.
- Common myths and mistakes that may compromise the strength of passwords.
- Review and consideration of effective administrative, physical, and technical safeguards to apply to your organization’s password management policy.

7



8

- Learn key criteria applicable to passwords that have the potential to contribute to a **higher level of security** with respect to the organization’s information system.
- Common **myths and mistakes** that may compromise the strength of passwords.
- Review and consideration of effective administrative, physical, and technical **safeguards** to apply to your organization’s password management policy.

8

Role Check!

9

Which is your area of focus?

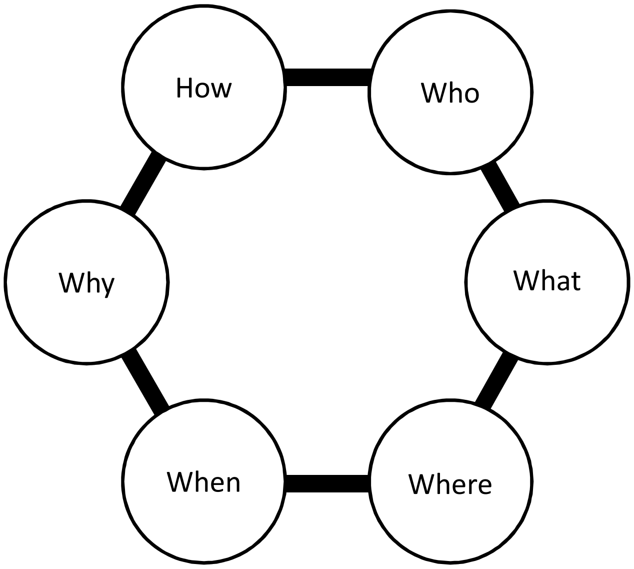
A. Privacy
B. Security
C. Compliance
D. Information Technology (IT)
E. Depends on the day

9

10

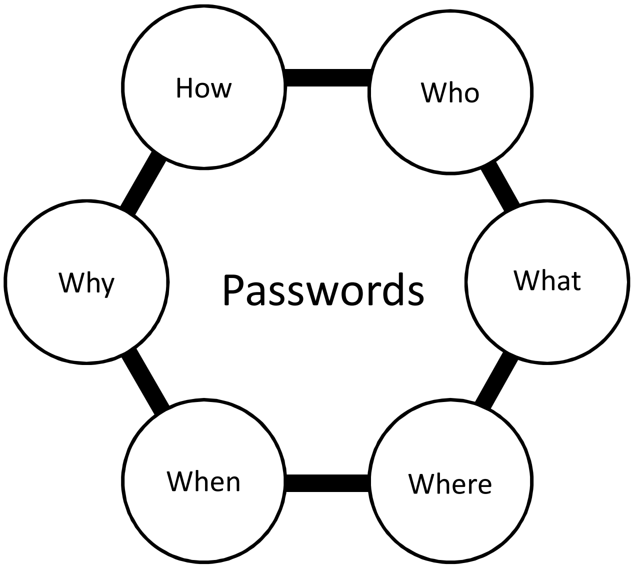
5WH1

10

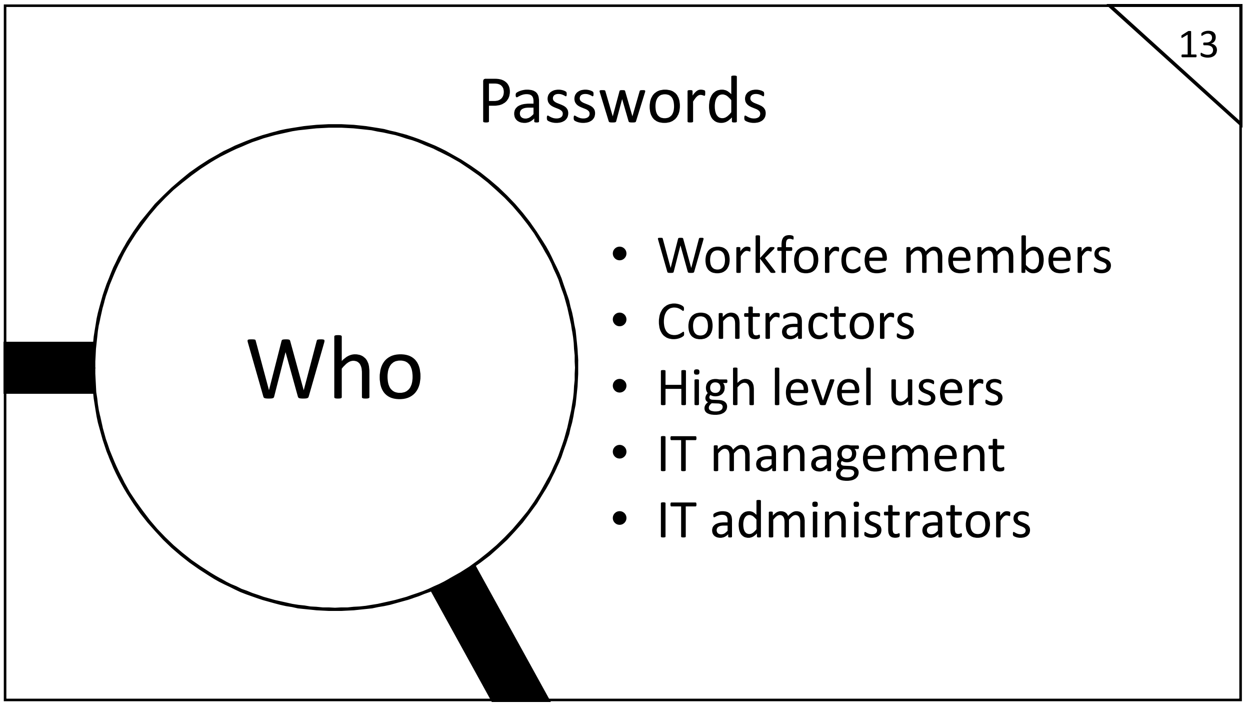

How
Who
What
Why
When
Where

5WH1

11


How
Who
Why
Passwords
What
When
Where

12



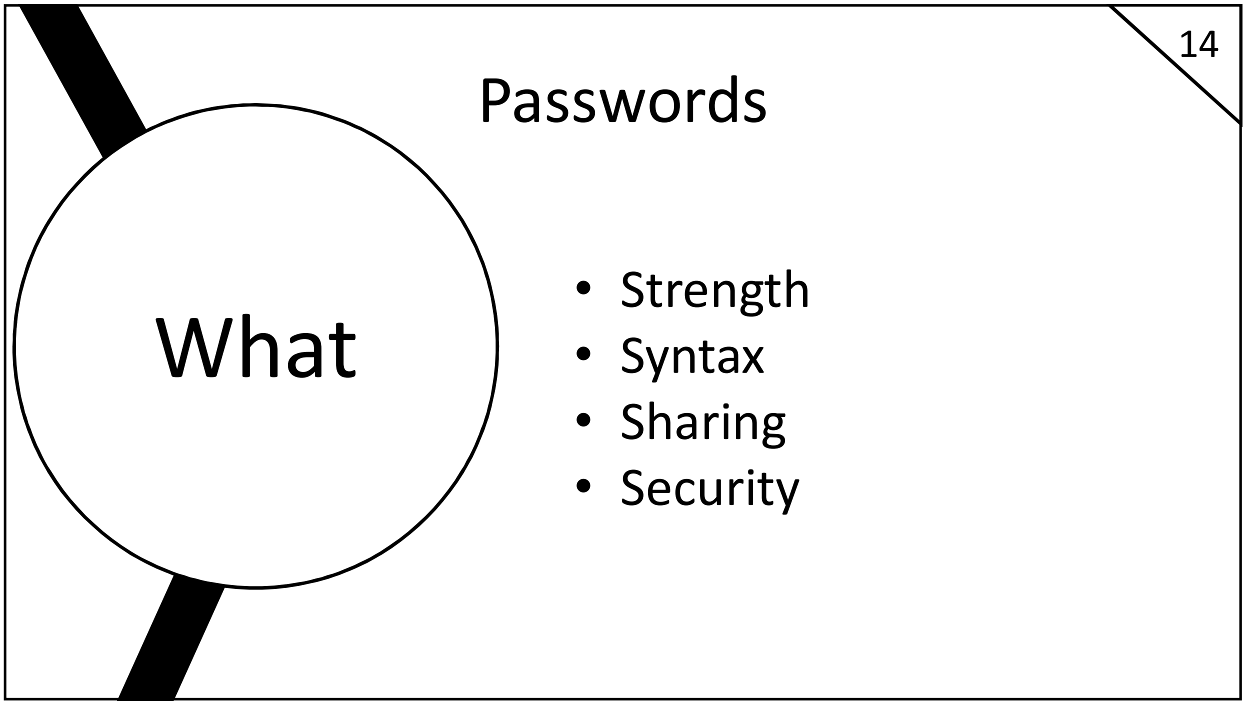
13

Passwords

Who

- Workforce members
- Contractors
- High level users
- IT management
- IT administrators

13



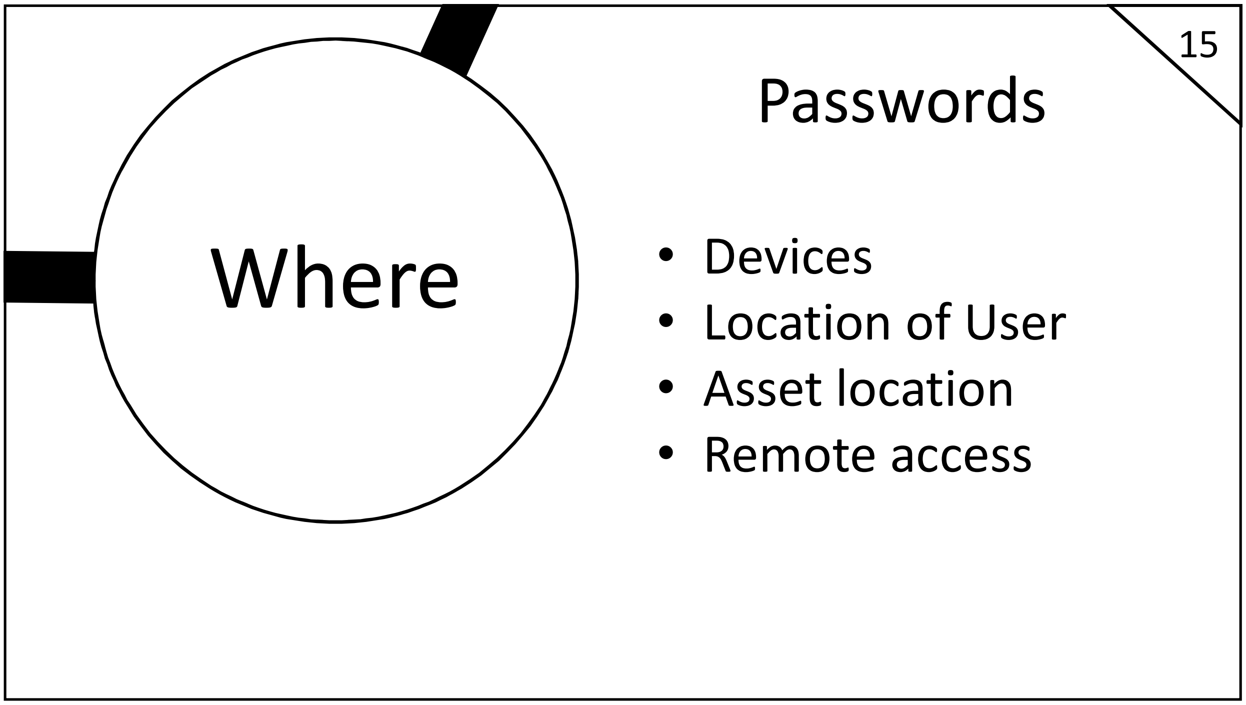
14

Passwords

What

- Strength
- Syntax
- Sharing
- Security

14



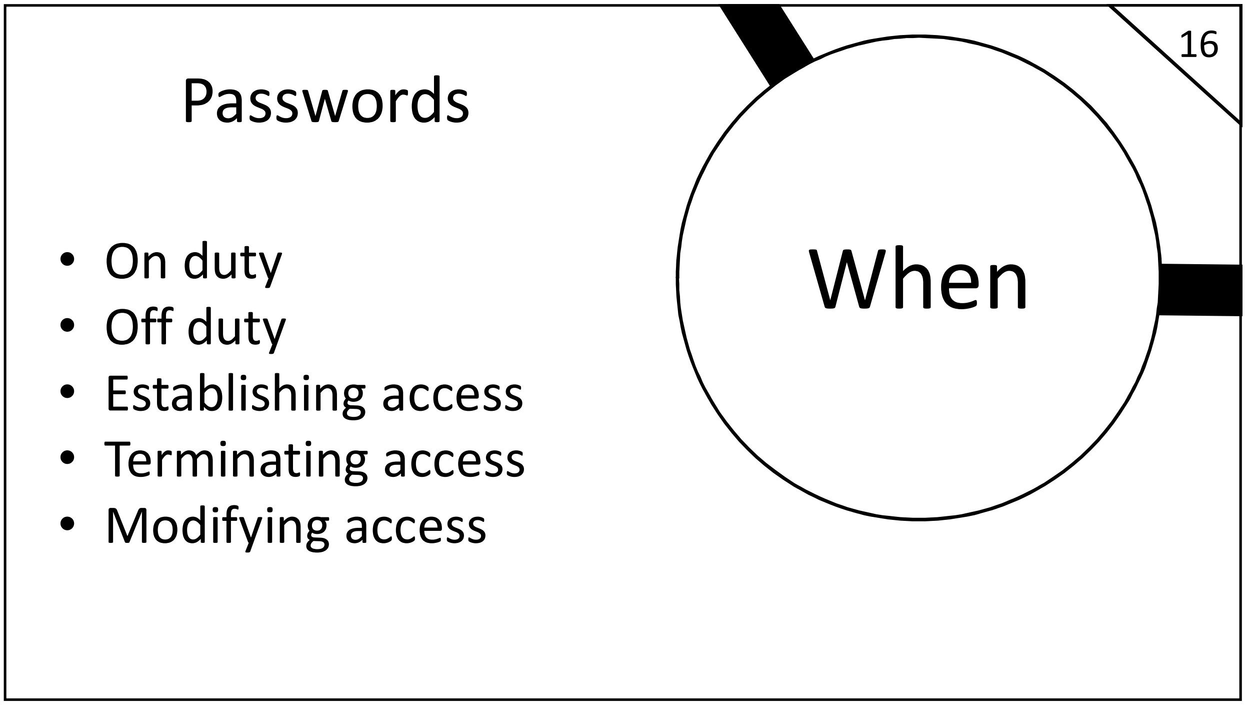
15

Passwords

Where

- Devices
- Location of User
- Asset location
- Remote access

15



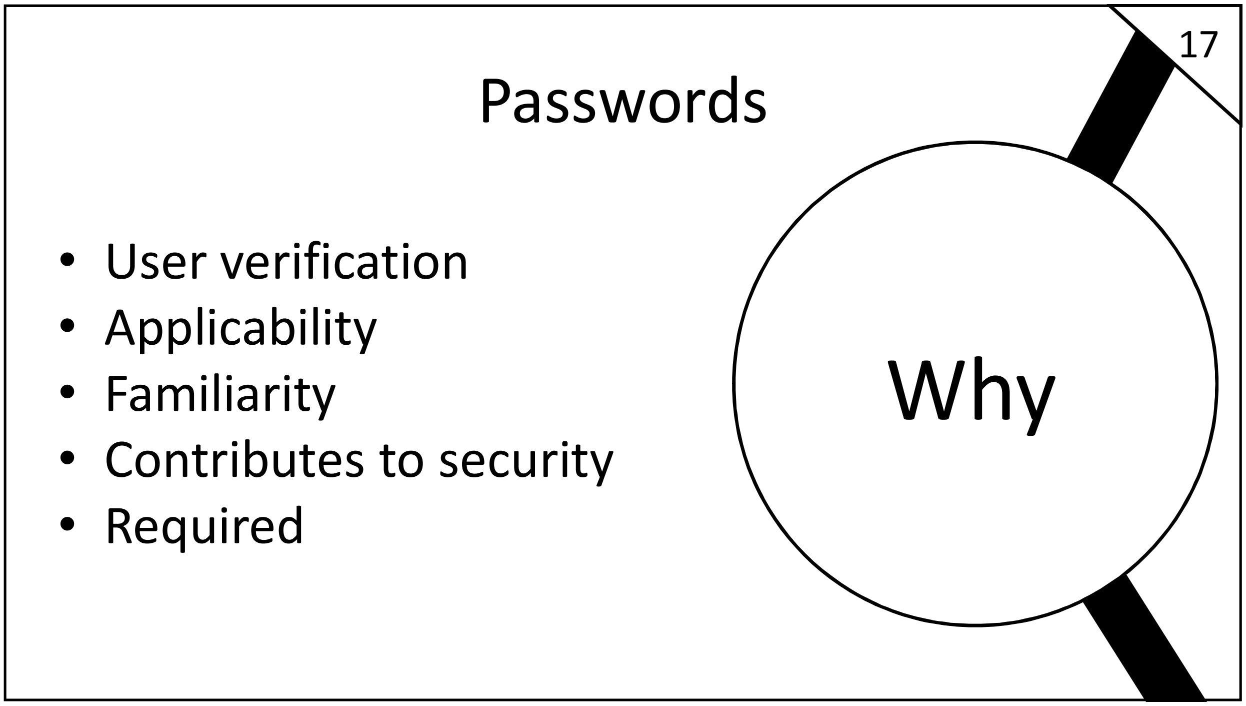
16

Passwords

When

- On duty
- Off duty
- Establishing access
- Terminating access
- Modifying access

16



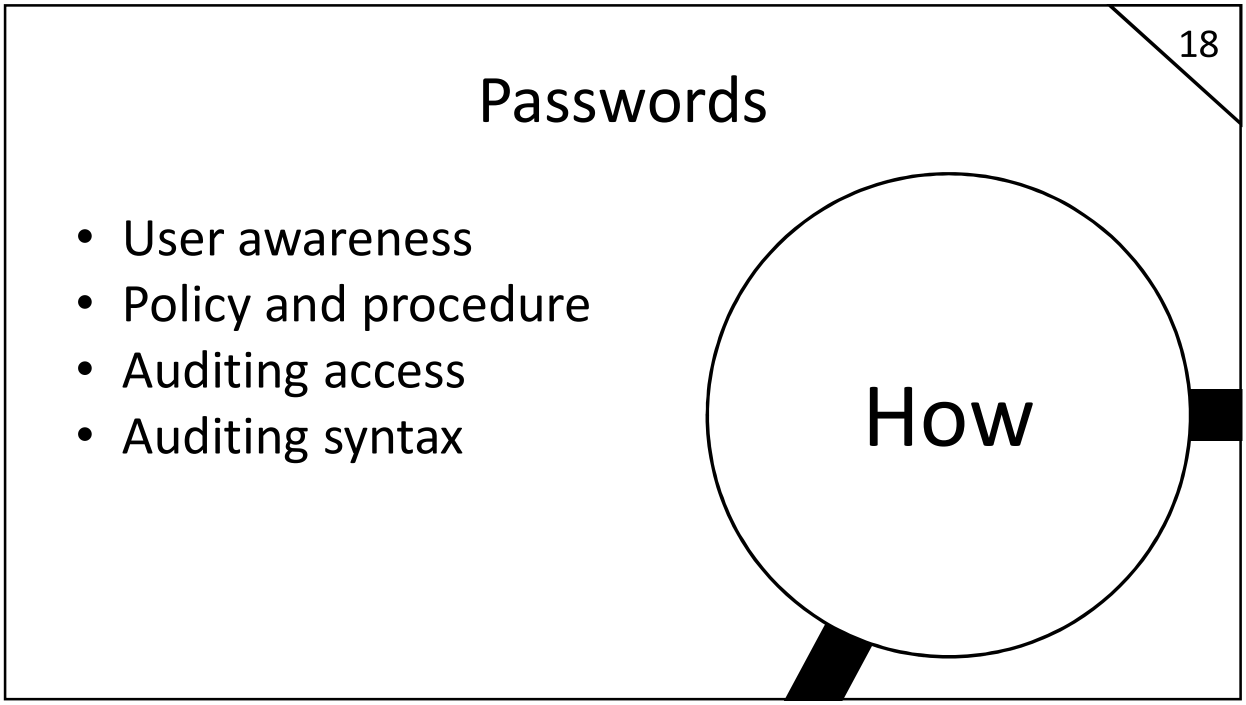
17

Passwords

- User verification
- Applicability
- Familiarity
- Contributes to security
- Required

Why

17



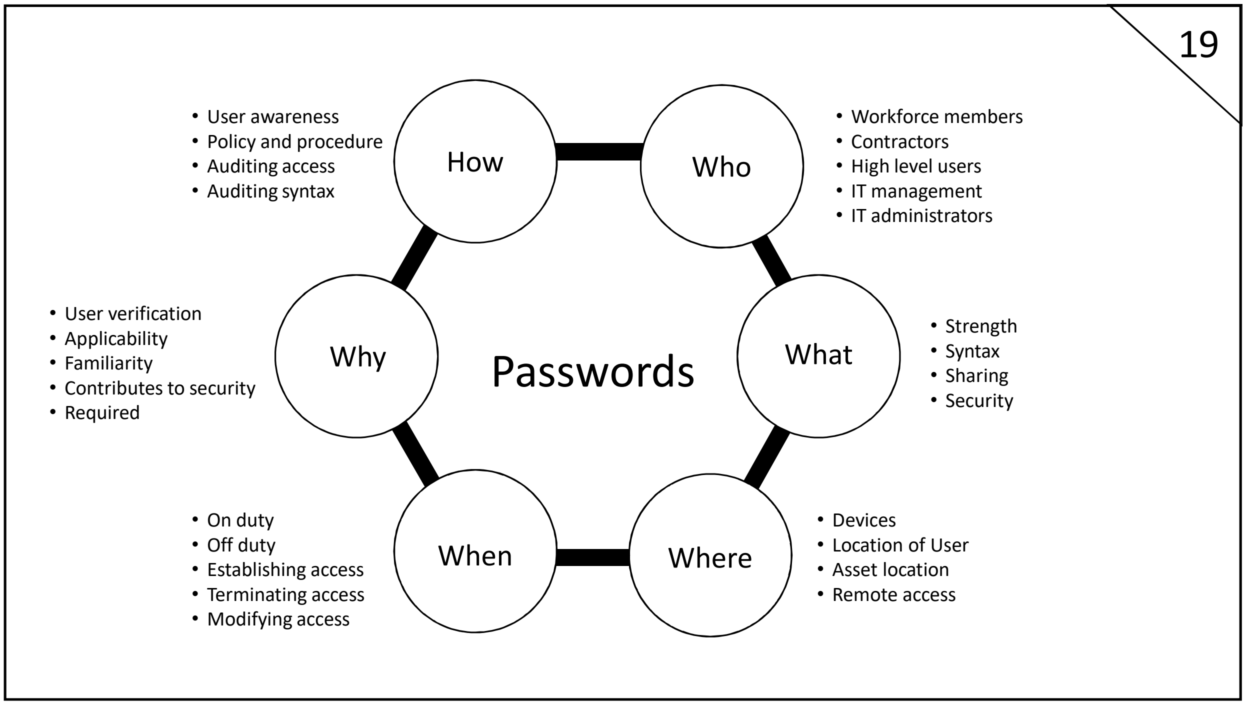
18

Passwords

- User awareness
- Policy and procedure
- Auditing access
- Auditing syntax

How

18



19

Passwords

How
- User awareness
- Policy and procedure
- Auditing access
- Auditing syntax

Who
- Workforce members
- Contractors
- High level users
- IT management
- IT administrators

What
- Strength
- Syntax
- Sharing
- Security

Where
- Devices
- Location of User
- Asset location
- Remote access

When
- On duty
- Off duty
- Establishing access
- Terminating access
- Modifying access

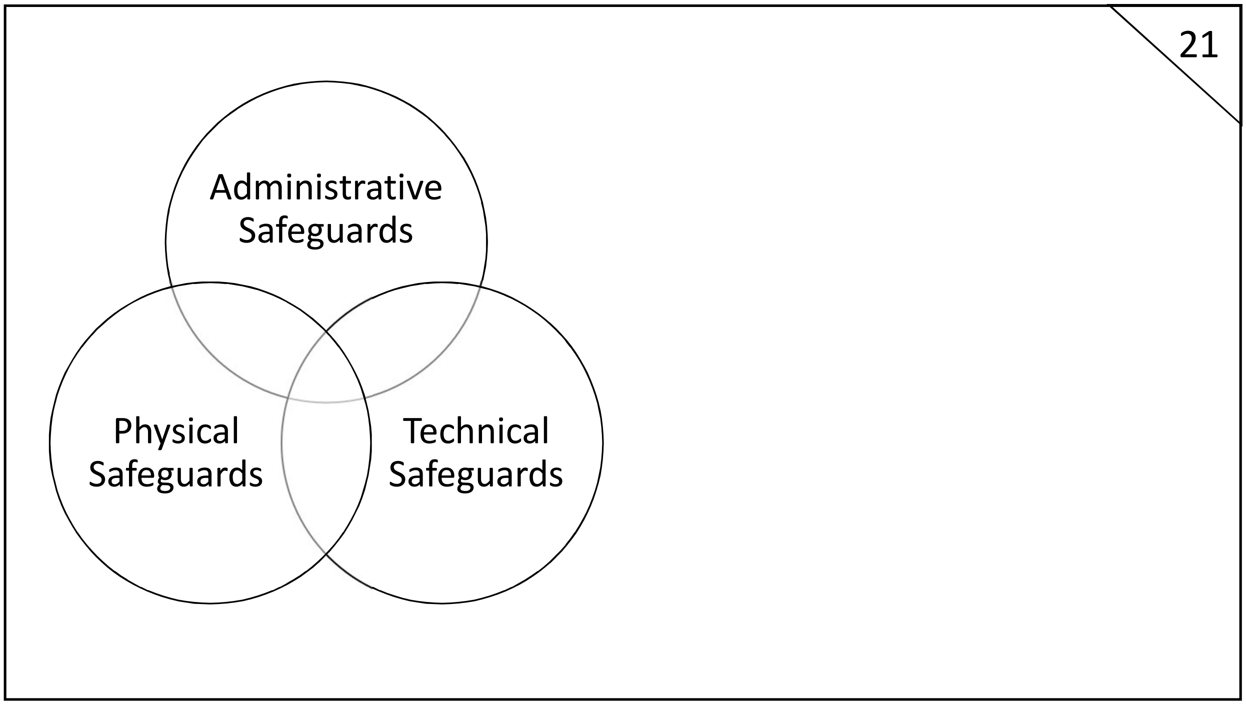
Why
- User verification
- Applicability
- Familiarity
- Contributes to security
- Required

19

20

Safeguards

20



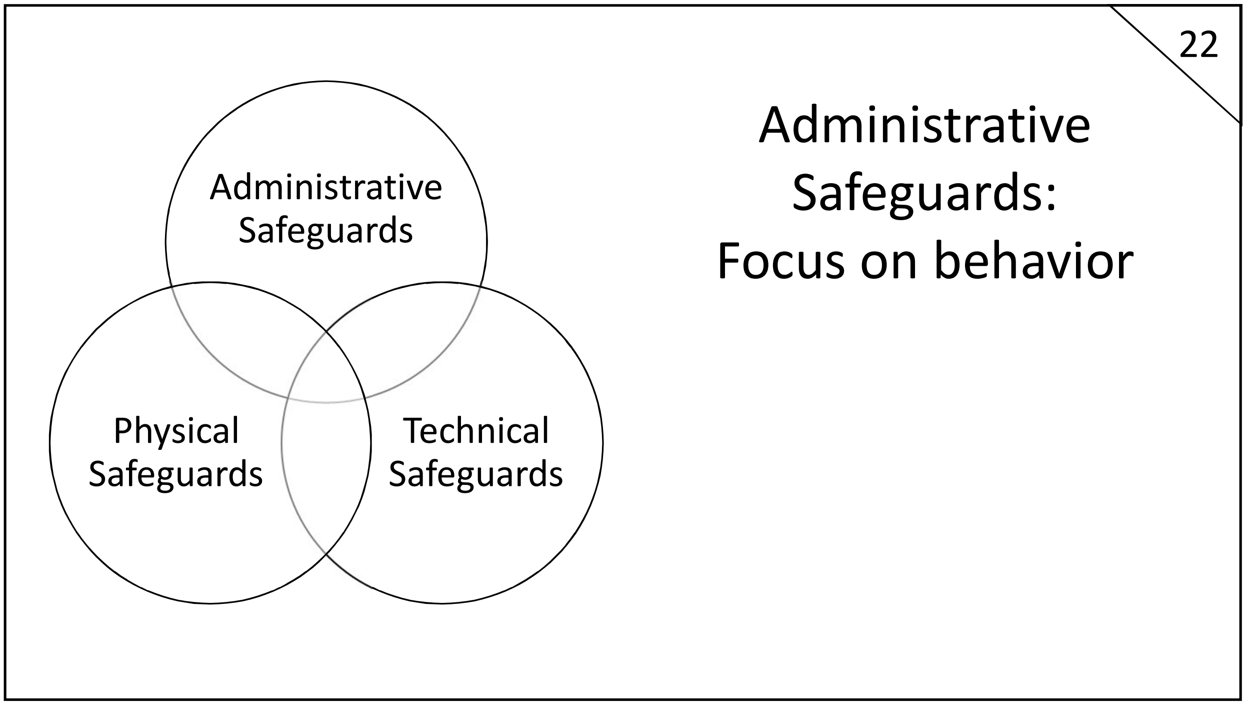
21

Administrative Safeguards

Physical Safeguards

Technical Safeguards

21



22

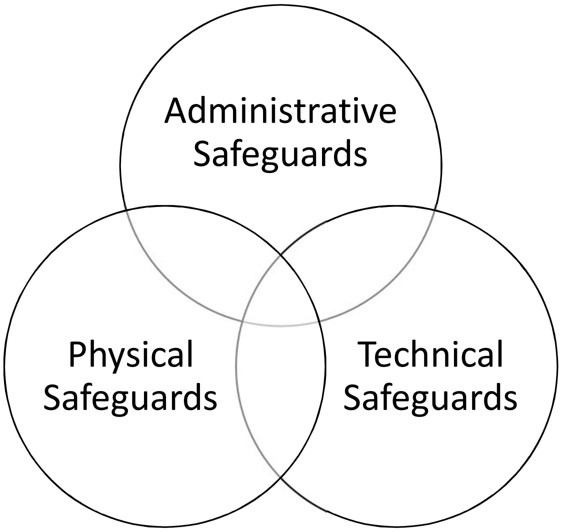
Administrative Safeguards

Physical Safeguards

Technical Safeguards

Administrative Safeguards: Focus on behavior

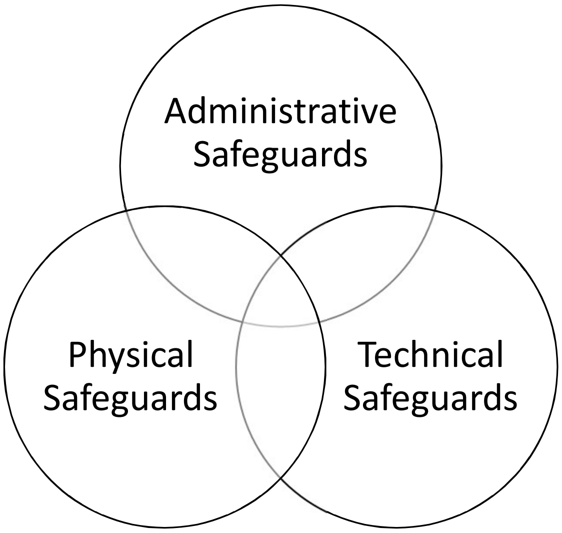
22



Administrative Safeguards: Focus on behavior

- Don’t share

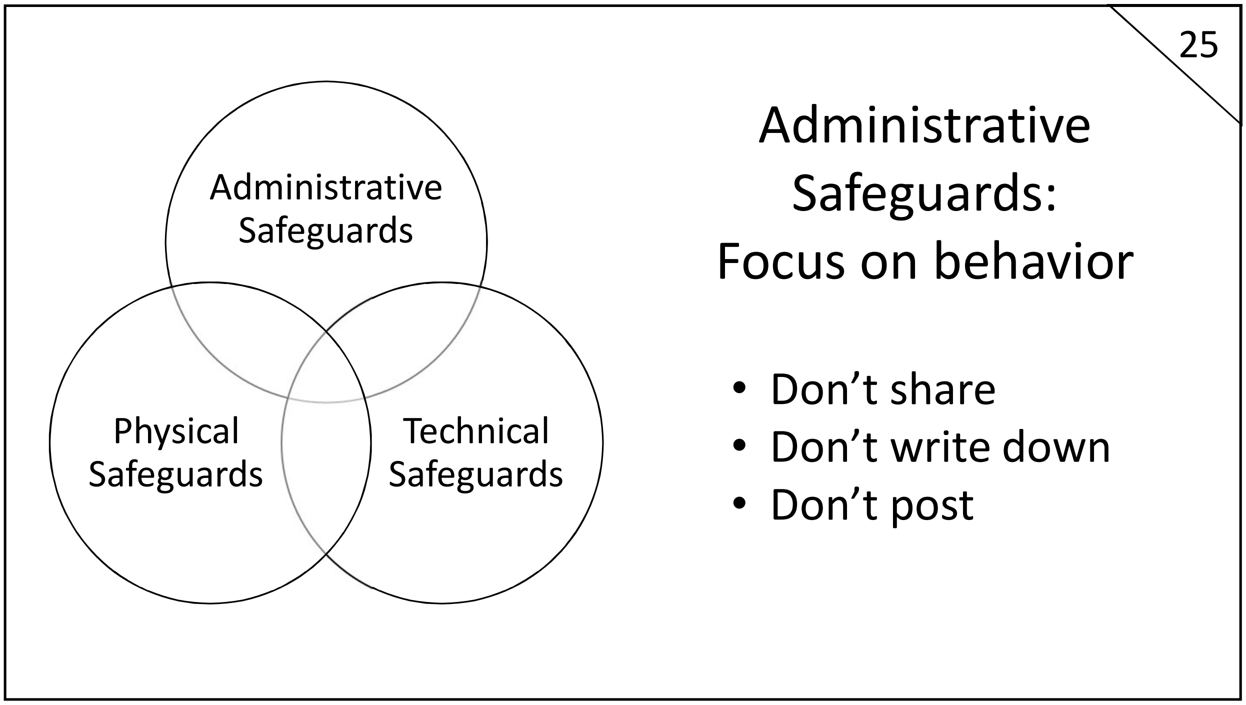
23



Administrative Safeguards: Focus on behavior

- Don’t share
- Don’t write down

24



25

Administrative Safeguards

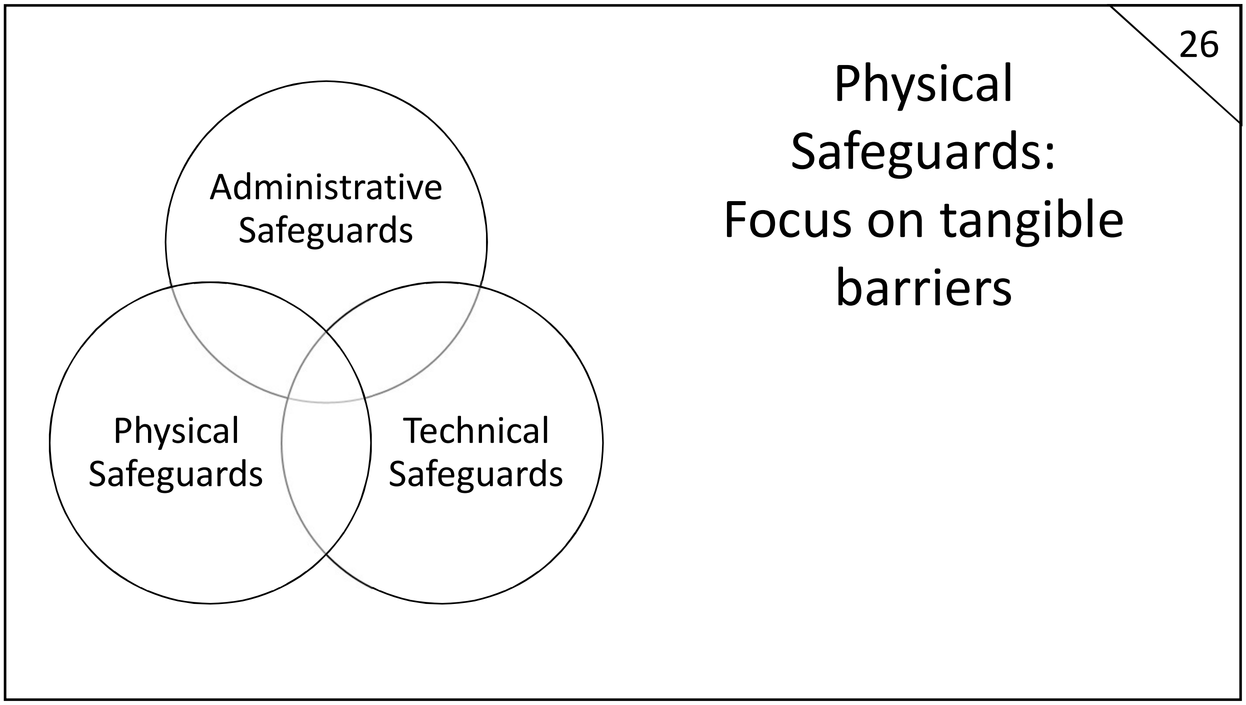
Physical Safeguards

Technical Safeguards

Administrative Safeguards: Focus on behavior

- Don’t share
- Don’t write down
- Don’t post

25



26

Administrative Safeguards

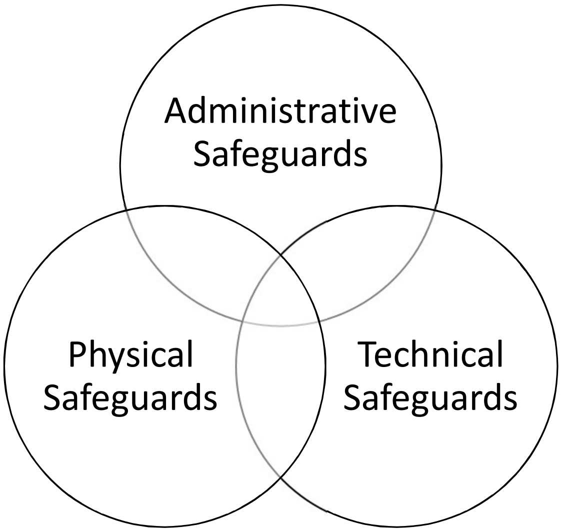
Physical Safeguards

Technical Safeguards

Physical Safeguards: Focus on tangible barriers

26

27

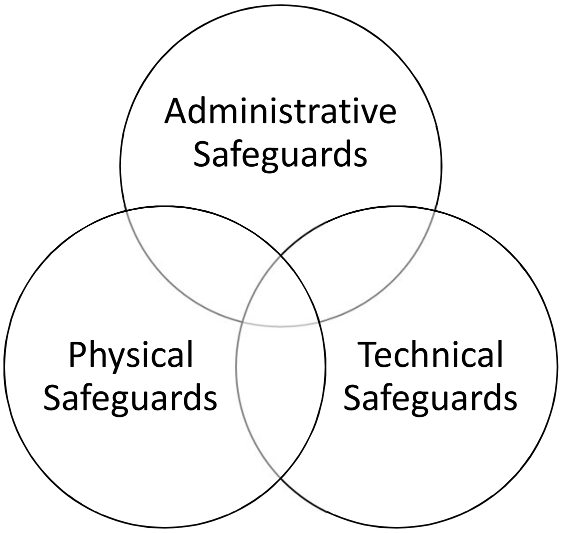


Physical Safeguards: Focus on tangible barriers

- Function activated

27

28



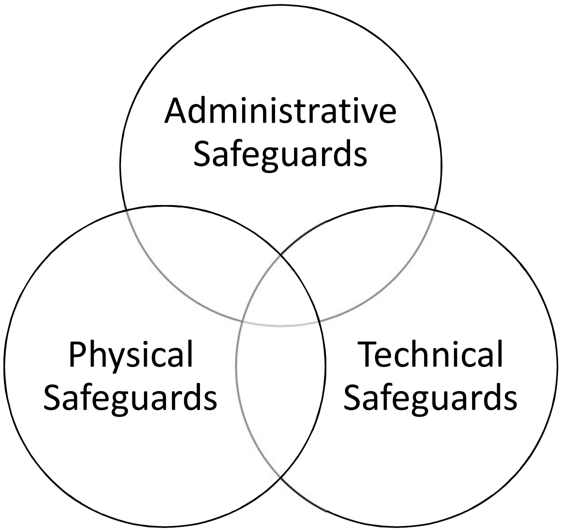
Physical Safeguards: Focus on tangible barriers

- Function activated
- Interface enabled

28

29

Technical Safeguards: Focus on use of technology

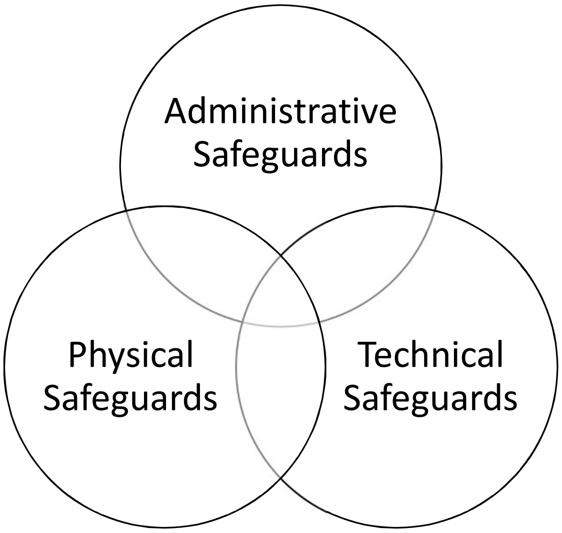


29

30

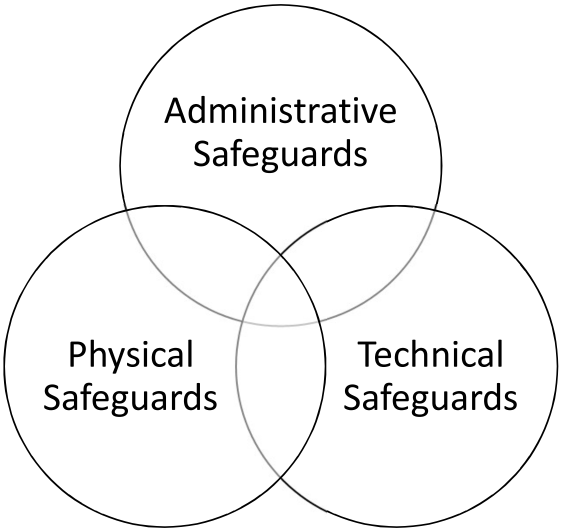
Technical Safeguards: Focus on use of technology

- Expiration date



30

31

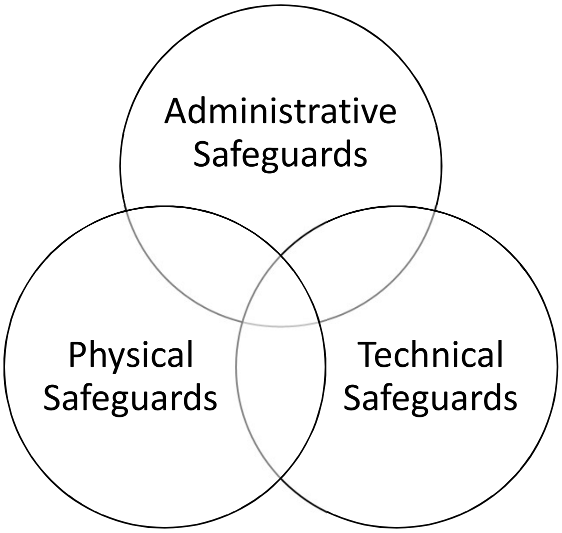


Technical Safeguards: Focus on use of technology

- Expiration date
- Syntax

31

32



Technical Safeguards: Focus on use of technology

- Expiration date
- Syntax
- Failed attempts

32

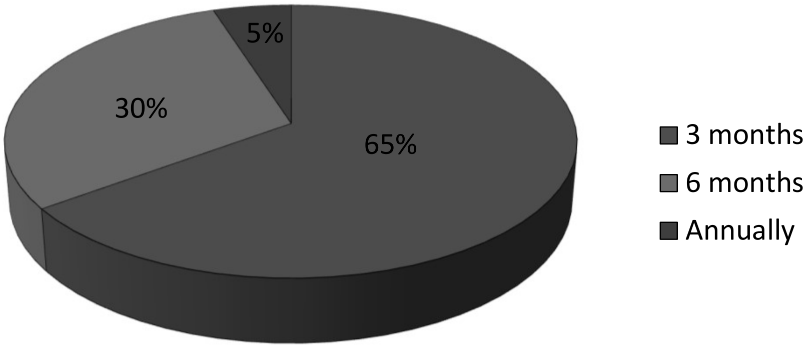
33

Changing Passwords

33

34

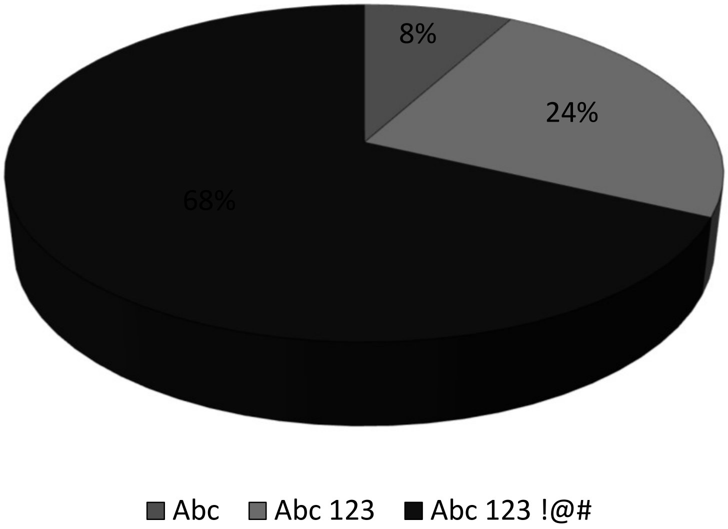
Frequency



34

35

Syntax



35

36

Strength

Mitigate the risk of someone guessing a password

36

37

Have you ever wondered?

- How many password combinations?
  - Consider the following
    - Letters – Capitalized – 26…25 for ease
    - Letters – Lowercase – 26…25 for ease
    - Numbers – All digits - 10
    - Special characters - 20

37

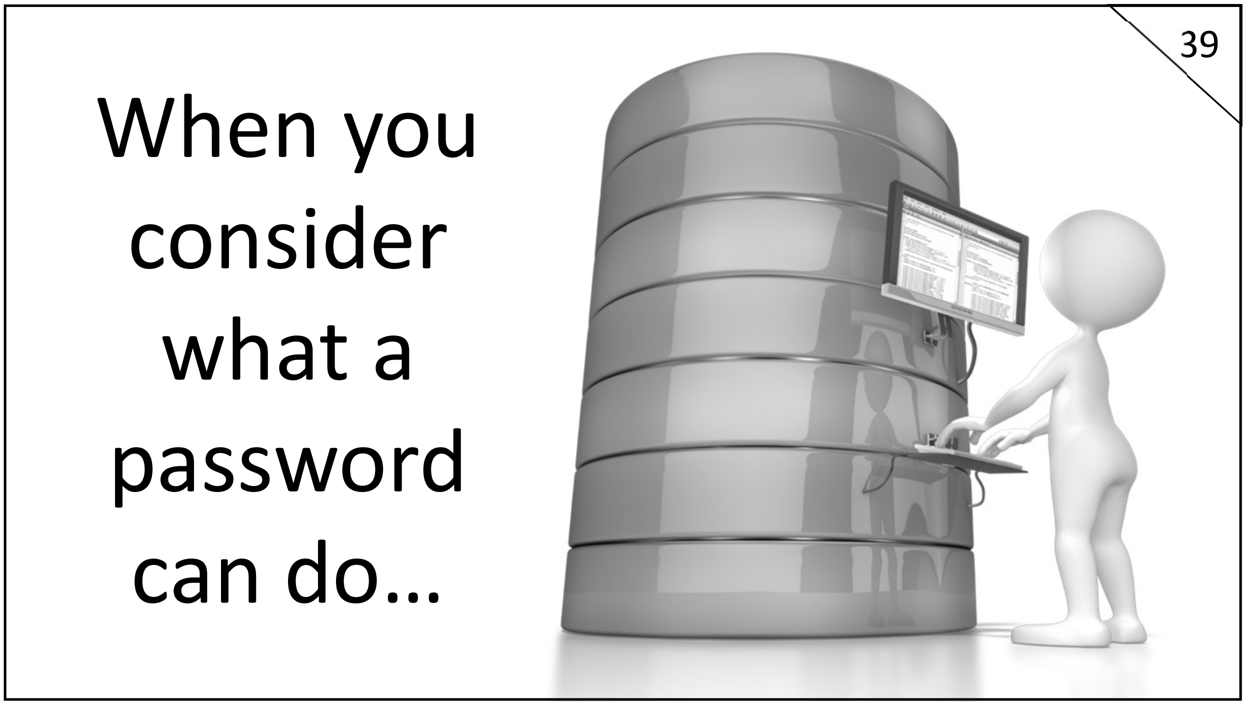
38

Have you ever wondered?

- 80 possible choices for each position
  - 4 characters – 40 million possible
  - 8 characters– 1.6 quadrillion

…I think you get the idea.

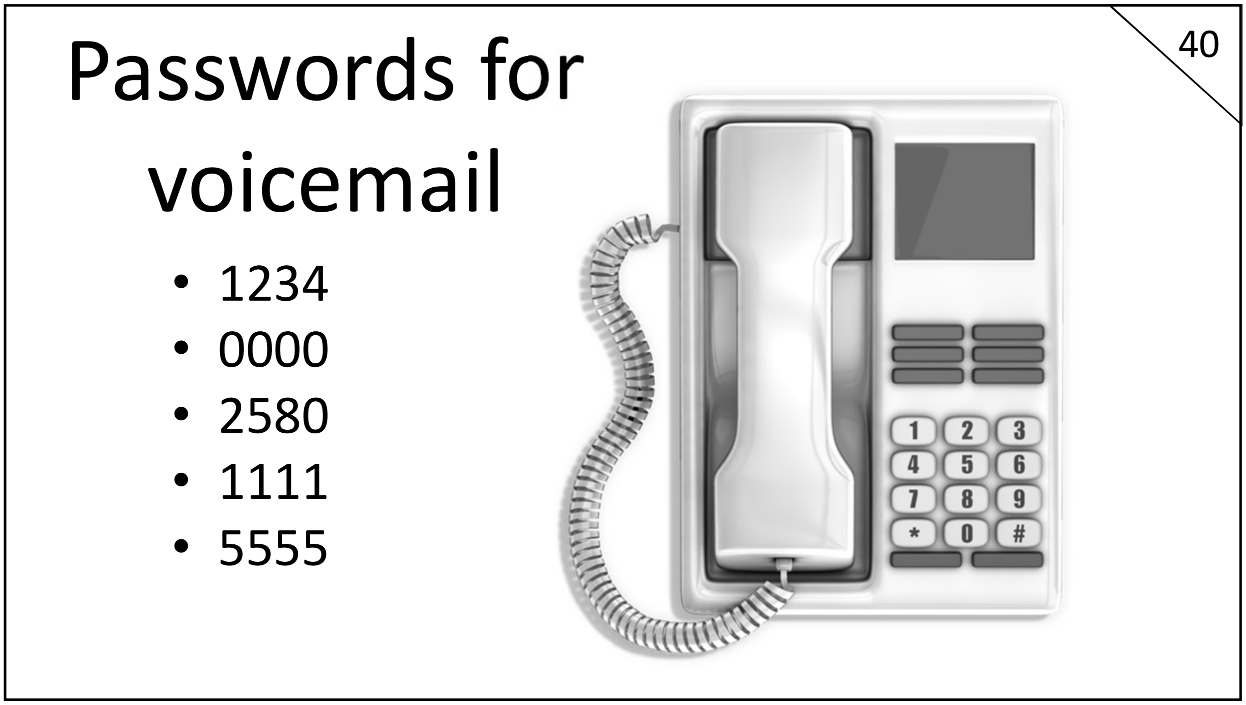
38



39

When you consider what a password can do…

39



40

Passwords for voicemail

- 1234
- 0000
- 2580
- 1111
- 5555

40

41

Next steps…

- Continued training
- Exercises
- Other threats : Social Engineering

41

42

Want to know…

- …how to check if an email's password was potentially compromised?
- …if a password was hacked?
- …how to decipher a password?

42

REVIEW
AND
Q&A

43