# CREATING A PGTS ELECTRONIC FILE STORAGE POLICY

AN EXAMPLE OF HOW TO IMPLEMENT STANDARD 23B

# LEARNING OUTCOMES

- Understand PGTS Standard 23b
- Learn best practices for electronic file security
- Learn best practices for electronic file backup
- Explore case studies where electronic files were exposed
- Work through Lake Union's process of creating a security and backup policy

# PGTS STANDARD 23

- “a. All physical files with current or potential fiduciary duties and all current legal documents are kept in properly secured fire-resistant files/vaults. All other fiduciary files and non-current legal documents are kept in safe and secure files.
- b. Electronic files held in a fiduciary capacity and other legal documents are properly backed up and secured per organizational policy approved by the governing board or committee and legal counsel. [PGP, PGTS]”

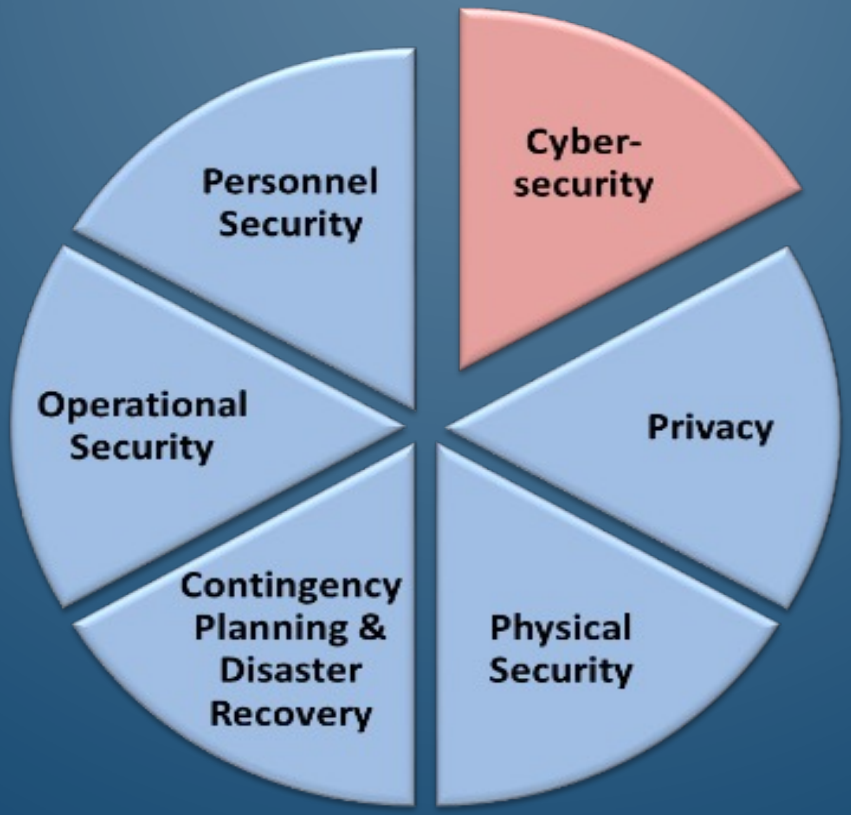
# WHAT IS INFORMATION SECURITY AND CYBERSECURITY

- Information Security is defined as ”the protection of information and information systems from unauthorized access, use, disclosure, disruption,  modification, or destruction in order to provide confidentiality, integrity, and availability
  - Confidentiality
  - Integrity
  - Availability
- Cybersecurity is formally defined as “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation”

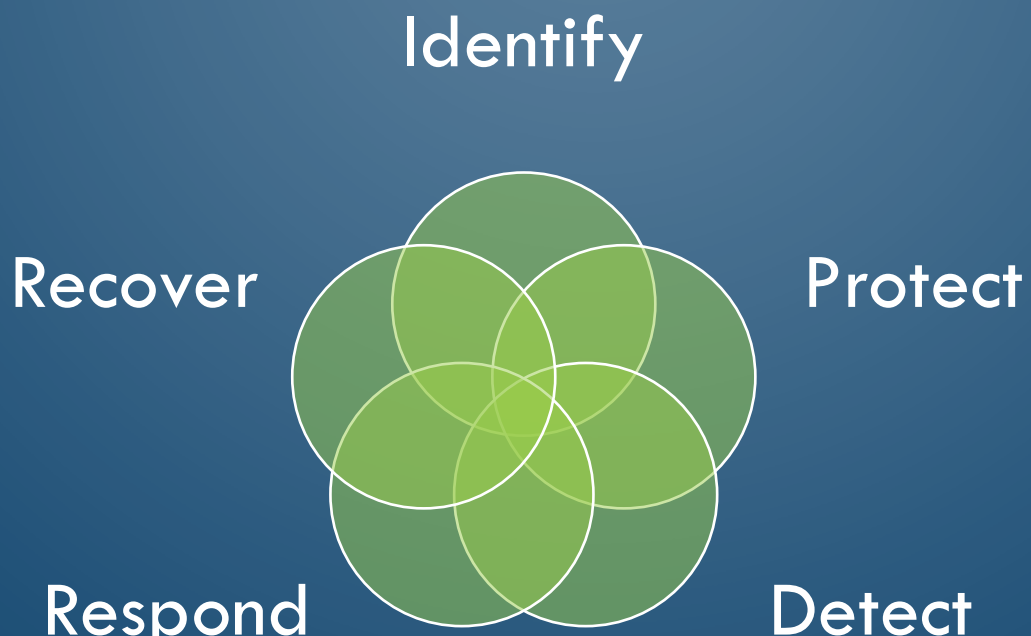
# IMPORTANCE OF ELECTRONIC FILE SECURITY AND BACKUP POLICIES

- To prevent
  - data breaches
  - Loss of documents and important files
  - Financial loss
  - Reputational loss
  - Exposing personal/confidential information
  - Unwanted copies of sensitive documents
  - Damage to information systems
  - Regulatory penalties and fines
  - Business disruption

# INFORMATION SECURITY



# SAFEGUARDING YOUR INFORMATION FRAMEWORK



# STEPS TO PROPERLY SECURING FILES

- Risk Assessment
- Data classification
- Manage/mitigate risks
  - Create an incident response plan
- Consider cyber insurance

# SECURITY BEST PRACTICES

- Digitize documents
- Use password protection
- Use strong passwords
- Set up MFA
- Encrypt files
- Avoid emailing sensitive/confidential files
- Backup
- Deletion versus destruction
- Determine which files to protect
- Create policies to implement these practices
- Perform a risk assessment

# WHY BACKUP?/ DATA LOSS CAUSES

- Database migration
- Software corruption
- Local disaster
- Ransomware attack
- Hard drive failure
- Theft
- Human error

# BACKUP CONSIDERATIONS

- Where?
  - Cloud v. local
- When?
  - Hourly, daily, weekly?
- How?
  - Full
  - Incremental
  - Differential
  - Mirror

# BACKUP CHALLENGES

- Data corruption
- Incomplete backup
- Insufficient storage capacity
- Slow backups
- Backup start or completion failure

# BACKUP BEST PRACTICES

- Backup regularly
- Select which data to backup
- Automate backups
- Test backup copies
- Policies should be reviewed and updated
- Consider encryption
- Use immutable storage
- Air gap business data
- 3-2-1 backups
  - 3: Create one primary backup and two copies of your data
  - 2: Save your backups to two different types of media
  - 1: Keep at least one backup file offsite

# CASE STUDIES

- Blackbaud Data Breach (2020)
- Hollywood Presbyterian Medical Center (2016)
- Little Red Door (2017)

# HOW LUC IMPLEMENTED 23B

- Assessed where we were
- Involved key stakeholders
- Determined the scope the policy we wanted to implement
- Determined how to get the policy approved by the “governing board or committee and legal counsel”

# LUC FINAL PRODUCT

- Limited to PGTS
- Key policy terms
- Expand to LUC-wide policy
- Lessons learned

# PARTICIPATION QUESTIONS

- How many of your organizations already have security and backup policies in place for electronic files?
- Who are some key stakeholders when developing an electronic security file?
- How often does your organization test your backups?