Congregation Data Security Education

Data Security Risks

- Incoming and Outgoing Internet Traffic
- Remote Access
- Outbound Email
- Improperly Discarded Paper
- Portable Media Devices (i.e., laptops, flash drives, CD's)

Data Security Defense

- Firewalls
- Routine Monitoring of Remote Users
- Internet Restrictions
- Identification and Classification of High-Risk Data
- Policies & Procedures Covering Use of High-Risk Data Residing in:
  - Desktop Computers
  - Emails
  - Paper Documents
  - Portable Media Devices (Disks, Flash Drives and Laptops)
  - Records Retention

Data Classification

- *Public* – Published Without Restrictions
- *Restricted* – Can be Shared at Owner's Discretion
- *Confidential* – Never Given to Anyone Outside the Four Walls of the Congregation (Personal Identity Information)

Personal Identity Information (PII)

Names & Addresses

Social Security Numbers

Credit Card Information

Documents with any Financial Information

Other Congregational Specific Information

Managing PII

Set employee systems access commensurate with job duties;

Review employee access on a periodic basis. Ensure all terminated employees' access have been removed & all active access is appropriate;

If temporary access is required, ensure it is revoked in a timely manner.

Do not download PII or confidential information unless it is absolutely necessary;

Set desktop screen to require a sign in after three minutes or sooner; and

Never leave reports containing this type of data in an unsecured area.

Where PII Resides

- Your Desktop Computer
- Email
- Remote Access
- Portable Media Devices (Disks, Flash Sticks. Laptops)
- Paper Reports
- Archive and Records Retention

PII on Your Desktop

Ensure confidential data residing on your desktop is protected by backup procedures.

Do not disable any passwords needed to access your desktop. Use hard to guess passwords for your personal login. *Do not share your password*!

Set your default security screen to automatically engage after three minutes of non-activity.

Never download PII unless it is absolutely necessary for the task at hand!

PII Contained in Email

Be aware that emails or attached documents can include PII. If not essential to the purpose of the email, do not include this information.

If PII is required, do not email PII or confidential data to any source, internal or external, unless *absolutely necessary*.

If the document must be emailed, add a password to electronic documents.

Remember, control of PII & Confidential Data is lost when emailed, unless it is password protected.

Remote Access to PII

- Create remote access policy & ensure all staff is educated in remote access use.
- Ensure remote access is critical to executing job requirements.
- If temporary access is required, ensure it is revoked in a timely manner.
- Remote access should be reviewed by management on a periodic basis to ensure all terminated employees have been removed and all active employee's access is appropriate.

PII Residing on Portable Media Devices

Identify the information to be downloaded.

Inform appropriate level of management of your intentions to download data and obtain permission.

If you have one, inform your tech support person to ensure all the downloaded data is properly protected by passwords or encrypted devices.

Eliminate all downloaded data when no longer needed.

Never download confidential or PII data onto a portable media device unless it is absolutely necessary to perform your job-related duties.

PII in Paper Form

Ensure that all print-outs containing PII or confidential data are stored in a ***locked*** file cabinet when not in use and shredded after no longer needed.

Do not print anything containing PII or confidential information unless it is absolutely necessary.

If a report containing this data needs to be distributed, ensure that it is distributed on a “need to know” basis and the recipient understands its confidential nature.

PII & Records Retention

Ensure all data that is no longer needed on site, but must be retained for a period of time, is sent to the archives or a secured location in a timely manner

Ensure ***all*** documentation no longer needed is shredded in the presence of a staff member.

Questions?

If you have any questions or suggestion about data security, please feel free to contact:

Helpdesk–(773)380-2472

helpdesk@elca.org