Subject:

Information Assurance and Security Policy

Policy:

The Board of Trustees has primary responsibility for establishing procedures and processes regarding use and security of informational technology in all WUMC facilities.

Procedure/Background/Other:

All members of WUMC community are responsible for protecting the security, confidentiality, integrity, and availability of information entrusted to them, and for taking affirmative steps to prevent unauthorized disclosure or loss. This policy sets forth the security requirements that all members of WUMC community must follow to meet that responsibility.

Approved On Behalf of the Board of Trustees by:

_____On_____

Contents

INFORMATION ASSURANCE AND SECURITY POLICY

Subject:

Information Assurance and Security Policy

Policy:

The Board of Trustees has primary responsibility for establishing procedures and processes regarding use and security of informational technology in all WUMC facilities.

Procedure/Background/Other:

All members of WUMC community are responsible for protecting the security, confidentiality, integrity, and availability of information entrusted to them, and for taking affirmative steps to prevent unauthorized disclosure or loss. This policy sets forth the security requirements that all members of WUMC community must follow to meet that responsibility.

Approved On Behalf of the Board of Trustees by:

_____On_____

I. AIM AND PURPOSE OF THIS POLICY

Williamsburg United Methodist Church (herein referred to as "WUMC") is entrusted with a great deal of information from members, employees, visitors, business partners, and other sources. That information is critical to WUMC's mission and to the administrative functions that support that mission. This information must have adequate safeguards in place to protect those it relates to and the organization.

All members of WUMC community are responsible for protecting the security, confidentiality, integrity, and availability of information entrusted to them, and for taking affirmative steps to prevent its unauthorized disclosure or loss. This policy sets forth the security requirements that all members of WUMC community must follow to meet that responsibility.

Who Does This Policy Apply To?

This policy is approved by the board of trustees and applies to:

- Our trustees, staff, members, volunteers, and anyone accessing Church Systems (defined below) (both paid and voluntary) or information contained on those systems, such as visitors, vendors, and contractors.
- Any individual involved in the collection or processing of personal data on behalf of WUMC.
- Any individual involved in the collection or processing of payments.
- All Church activities, whether on campus or off, and to all information regardless of the medium in which it is stored (paper, electronic, etc.) or shared (electronically, verbally, visually, etc.).

Violations of this policy may result in disciplinary action up to and including separation from

WUMC.

II. Definitions

Information generated, collected by, or entrusted to WUMC is classified as follows:

Confidential Information

Confidential Information means data that is protected by federal, state or local law or contractual obligation, or that is specifically designated as confidential by WUMC. Information also is considered confidential if its loss, misuse or unauthorized disclosure or alternation might cause substantial injury to

WUMC and/or its members in terms of financial loss, reputational damage, operational capability, and/or significant embarrassment. Examples of Confidential Information include, but are not limited to:

- PII
- HIPPA
- Pastoral Care
- Payroll records
- Personnel (employment) records
- Bank account, credit/debit card or other financial information

The highest levels of security must be applied to restrict access to confidential information to authorized individuals, and to protect against its unauthorized use, disclosure, or modification.

Personal Data

Personal Data means all data that is not classified as either "Confidential" or "Public" and its loss, misuse or unauthorized disclosure or alteration might cause moderate injury to WUMC and/or its members. Examples include, but are not limited to:

- Internal directories
- Contact Information (full name, email address, mailing address, phone number)
- Non-public meeting minutes or memoranda
- Contracts
- Information about financial transactions
- Drafts of official documents
- Employee Social Security numbers

A reasonable level of security must be applied to limit access to Personal Data, and to prevent its unauthorized use, disclosure, or modification.

Public Information

Public Information means data that is open to WUMC community, external entities, and the general public. Examples of Public Information include, but are not limited to:

- Press releases
- WUMC website
- Publicly posted schedules or calendars
- Publicly posted or published newsletters or magazines

A reasonable level of security within the industry standard must be applied to protect Public Information against unauthorized modification.

Custodian

Custodian means any individual who has been approved to execute a Legitimate Business Function which requires the provision of access to Restricted Church Information, or who uses that information in support of a Legitimate Business Function.

Data Steward

Data Steward means a Church official with enterprise responsibility over Restricted Church Information.

Legitimate Business Function

Legitimate Business Function refers to the justification, as approved by an appropriate supervisor, for which access to Restricted Church Information is approved.

Mobile Device

Mobile Device means an electronic device, without regard to ownership, that is easily transportable and capable of accessing, storing, or transmitting information. Mobile devices include but are not limited to laptop computers; tablets; netbooks; cell phones; Smartphones (e.g., iPhones, Galaxy); flash or "thumb" drives; magnetic tape; discs; and external hard drives.

Personally Identifiable Information (PII)

(PII) is information that, when used alone or with other relevant data, can identify an individual.

Restricted Church Information

Restricted Church Information means any information which is classified by WUMC as either Confidential or Internal Use (see the definitions above).

Church Systems

Church Systems means Church-owned or controlled computing devices, data networks, software, databases, services, and facilities. Examples of Church Systems include but are not limited to shared computer drives, network file shares, networkable copiers, Church-provided wireless networks (WiFi), and Church-provided programs or software such as Microsoft Word, Outlook, Amplify, Canva, Mailchimp, Adobe Suite and Zoom.

III. Expectation of Privacy

Communications and information transmitted, and activities conducted with regard to the operations of WUMC are expected to be monitored.

COLLECTION OF PERSONAL DATA

Williamsburg United Methodist Church will only obtain Personal Data in support of its objectives through lawful and fair means and with the knowledge and consent of the individual concerned. Such consent for the collection, processing, and / or transfer of their Personal Data will be established through the following principles:

- Ensuring that the request for consent is presented in a manner which is clearly distinguishable, using clear and plain language.
- Ensuring the consent is freely given.
- Documenting the date, method, and content of the consent, in addition to its intended use.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

Consent may be provided electronically, or in writing.

As minors are unable to consent to the Processing of Personal Data, consent must be sought from the person who holds parental responsibility over the minor.

DATA PROCESSING

WUMC uses the Personal Data it collects for the following broad purposes:

- The general running and administration of WUMC.
- To fulfill the objectives of WUMC, including the provision of pastoral care to its attendees

The use of Personal Data will be considered from the data subjects' perspective – considering whether its use for the intended purpose would align with the consent under which it was provided.

In any circumstance where consent has not been expressly provided for specific activity being completed, one or more of the following conditions must be satisfied to determine the fairness and transparency of any further processing:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further processing.
- The context in which the Personal Data has been collected, in particular the relationship between the data subject and the data controller.
- The possible consequences of the intended further processing for the data subject.
- The existence of appropriate safeguards relating to further processing, which may include encryption, anonymization or pseudonymization.

DATA QUALITY

WUMC will adopt all necessary measures to ensure that the Personal Data it collects and processes is complete and accurate in the first instance and is updated to reflect the current situation of the data subject.

The measures adopted by WUMC to ensure data quality include:

- Correct Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Inactivate, rather than delete Personal Data where:
    - The law prohibits erasure
    - Erasure would impair the legitimate interests of the Data Subject ○ The data subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

WUMC will request on a periodic basis that data subjects ensure that personal data is accurate and complete.

IV. System Access Requirements

Limiting access to Church Systems can prevent unauthorized access to those systems and the information they contain. WUMC therefore provides limited access to those systems based upon a demonstrated business need. Access to Church Systems requires the following:

A. An authorized relationship with WUMC (i.e., staff, members, and in limited circumstances vendors or contractors);
B. A Legitimate Business Function as certified in writing by the individual's direct supervisor;
C. A completed system access agreement;
D. Approval for access to information domains by the relevant Data Steward; and

E. Use of a unique username and password by each individual granted system access (group access and shared credentials may be permitted on an exception basis with the approval of the CIO.) See the Information Security Requirements, below, for the required steps for protecting credentials.

Access is conditioned upon the user's agreement to abide by the foregoing requirements and all applicable Church policies.

V. Responsibilities

All members of WUMC community share the responsibility for safeguarding Church information.

The following individuals/offices have a heightened expectation as outlined below:

A. Data Steward: Responsible for the decision to authorize, or not, access to Restricted Church Information for which they are the primary Church executive in charge of that functional area (e.g., Finance: Chair of Finance Committee / Membership: Business Manager and Director of Congregational and Community Engagement [Communications]).

B. Data Custodian: Responsible for the security of Restricted Church Information to which they have been granted access, in whatever format (e.g., electronic, paper, verbal).
    1. Access to member PII is granted to the following:
        a. Staff
        b. Connection Corner Volunteers
        c. Committee Chairs
    2. Access to Financial Data
        a. IAW Finance Committee

C. Technology Services IT Service Provider: Responsible for the implementation and auditing of functional controls which support the restriction of access to Restricted Church Information to individuals with a Legitimate Business Function that has been appropriately approved for such access.
D. Department Head: Responsible for ensuring that Restricted Church Information is appropriately handled, stored, and destroyed in accordance with applicable Church policy.

VI. Information Security Practices

All staff are responsible for completing WUMC's mandatory online Privacy and Information Security Training. All members of WUMC community, and anyone accessing Church Systems, are responsible for adhering to WUMC information security requirements, including but not limited to the following:

Protect System and Network Access

1. Know and follow the requirements in WUMC's Technology Use Policy.
2. Do not use Church systems in a way that negatively impacts the functioning or availability of those systems.
3. Treat credentials for access to Church systems (e.g. usernames and passwords) as confidential. Such credentials are non-transferable and should never be shared, *even with Church personnel from Technology Services.*
4. Use strong passwords to access Church systems and to secure personal computers.
    a. Minimum of 8 characters and must contain (1) each of the following; capital letter, number, special character
5. Do not write down passwords where they are easily accessible to others.
6. Do not save passwords in Church web browsers or send via e-mail.
7. Do not attempt to access Church systems unless authorization has been provided (see System Access Requirements, above).
8. Log out from a Church system when you are finished working, or if you will be away from your computer for more than a few minutes.
9. Maintain up-to-date anti-virus software and system patches on all computers. When prompted to update such software or patches do so as soon as possible.
10. Do not download or install computer programs or software onto Church Systems without prior approval from Technology Services (TS).
11. Access Church systems and Restricted Church Information only on Church provided or specifically approved hardware.

Protect the Confidentiality of Information

1. Do not share information collected for a specific purpose with those outside WUMC community without notification and consent.
2. Do not access or use Restricted Church Information other than for a Legitimate Business Function.
3. Do not share Restricted Church Information with those who do not have a Legitimate Business Function which requires knowledge of that information.
4. Fax/Scan confidential data only after confirming that the receiving machine is located in a secure area accessed only by those with a legitimate need to see the information being transmitted.
5. Do not leave paper documents containing Restricted Church Information where they are accessible to those who do not have a legitimate need to know that information. Secure all such documents in a locked suite, office, desk, or file cabinet.

6. Store Confidential Information only on an appropriately encrypted medium. Contact our Information Technology Service Provider to have the necessary encryption technology installed on your computer.

Protect the Integrity of Information

1. Do not modify Church information for purposes other than a Legitimate Business Function.
2. Do not use Church information for personal use or benefit.
3. Do not infringe or alter the intellectual property of others.

Take Care with E-mail

1. Adhere to the requirements in the WUMC Electronic Communications Policy.
2. Do not use personal e-mail for work purposes.
3. Do not download e-mail attachments or click on links from unknown senders. Be cautious of emails from known senders that appear suspicious or out of character.
4. If using a mobile device, follow the Additional Requirements for Mobile Devices, below.

Dispose of Information and Equipment Properly

1. Shred all written documents that contain Restricted Church Information when they are no longer required.
2. If you are unsure whether you are authorized to access, share, or transmit confidential information, or have other questions about protecting that information, contact the Business Office for guidance.

Additional Requirements for Off-Campus Computing

Employees who work from off-campus locations must take additional steps to protect information, including use of an encrypted communication channel to access Church systems and information. Before accessing such systems or information see the Telecommuting Policy and contact our Information Technology Service Provider in order to implement the required security measures for off-campus computing.

VI. Report Potential Information Security Breaches

Any individual who suspects that a Breach of WUMC Systems has occurred due to the theft or exposure of Personal Data or Confidential Data must immediately notify the Business Manager, providing a description of what occurred.

All reported incidents will be investigated to confirm whether or not a Breach has occurred. If a Breach is confirmed, WUMC will follow the established protocols based on the criticality and the scope of the Breach. The Chair of the Board of Trustees shall be notified of any confirmed Breach.

APPENDIX 1: INFORMATION SECURITY POLICY ACKNOWLEDGEMENT

Volunteer Name (Print):

I agree to take all reasonable precautions to ensure that sensitive information entrusted to Williamsburg United Methodist Church will not be disclosed to unauthorized persons.

I understand that I am not authorized to use Confidential or Personal Data obtained by WUMC for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of a trustee.

I have access to a copy of the Information Security Policy, I have read and understand it, and I understand how it impacts the areas I operate within.

I agree to abide by the policies and other requirements found in the Information Security Policy. I understand that non-compliance may lead to criminal and / or civil penalties.

I also agree to promptly report all violations or suspected violations of this Information Security Policy to the Business Manager.

Signature: _____

Print Name: _____

Date: _____

Concerns, Complaints, And Compliments

Should anyone have any concerns, complaints, or feedback in relation to this policy please contact:

Name: _____

Telephone Number: _____

Email Address: _____

It would be helpful to have complaints in writing as this avoids any possible misunderstanding. Whether verbal or in writing, complaints will be acted upon at the earliest convenience. The target response for written complaints is 10 days.

Document Review

The trustees will review this policy annually, amending and updating it as required. Communication of changes will be distributed to those affected.

Date of Most Recent Review: _____

Date of Next Review: _____

Signed (on behalf of Church Trustees): _____