**Technology and Data Security Policy**

**July 19, 2019**

**Scope**

This Technology Policy (“Policy”) applies to the Presbyterian Church (U.S.A.), A Corporation and its Constituent Corporations including the employees designated to the Presbyterian Mission Agency (“PMA”), the Office of the General Assembly (“OGA”) (hereafter collectively the “A Corporation”), the Presbyterian Church (U.S.A.) Investment and Loan Program, Inc. (“PILP”), Presbyterian Women in the Presbyterian Church (U.S.A.), Inc. (“PW”) and any other related entity and the employees, volunteers, and independent contractors of any of them (hereinafter collectively “Related Entities”) (collectively hereinafter called “Users”), that use Computing Assets belonging to the A Corporation or that contract for the services of Information Technology (“IT”). This Policy also applies to anyone who accesses the A Corporation’s systems and computer networks by using any physical or virtual item, device, software or other methods to connect to Computing Assets.

Outside Contractors/Consultants

All contractors/consultants to the Related Entities that use Computing Assets or which contract for the services of IT will be given a Packet containing A Corporation policies. These persons/companies will agree, in writing, to abide by the terms outlined in the Packet, including granting IT the right to audit and remove software if necessary, as a condition of continued use.

 Volunteers

All volunteers who serve the A Corporation, who are granted access to Computing Assets owned by the Related Entities, will be provided with a Volunteer Compliance Packet containing A Corporation policies. These persons will agree, in writing, to abide by the terms outlined in the Packet, including granting IT the right to audit and remove software if necessary, as a condition of continued use.

**Definition of Computing Assets**

“Computing Assets” include the following physical and virtual items owned by or licensed to the A Corporation for the benefit of the Related Entities including:

* Desktop and laptop computers and devices
* Software (licensed commercial software, freeware, shareware, open source software, demonstration software, custom software)
* Operating systems
* Data
* Internet access, both wired and wireless
* Printers, including multifunction copiers
* Scanners
* Other computer peripherals
* Networking equipment
* Servers, physical, virtual, cloud-based
* Cabling
* Telephone equipment
* Fax Equipment
* Mobile devices including, but not limited to, smartphones and tablets
* Removable storage devices including, but not limited to, thumb drives and removable hard drives
* Other items that connect to A Corporation networks

This Policy also applies to any consulting or contract work intended to result in the planning, purchase, creation, or deployment of Computing Assets, the service of A Corporation volunteers who are permitted to access Computing Assets, and technology services including Internet and telecommunications services and maintenance contracts that involve Computing Assets.

**Ownership of Computing Assets**

Computing Assets

All Computing Assets purchased by IT for the A Corporation are the property of the A Corporation.

All Computing Assets purchased by the Related Entities are the property of the Related Entities (“RE Computing Assets”). To the extent that RE Computing Assets are managed and served by IT, they will be managed according to this Policy, and any Service Level Agreements. Related procedural documents used by IT also serve to clarify ownership of Computing Assets and RE Computing Assets.

All Other Technology Assets

All resources and assets such as software developed by A Corporation employees in the course of their employment are the property of the A Corporation unless otherwise approved in writing by officers of the A Corporation and a Related Entity. Any contracts for development of technology assets or resources including software development for the A Corporation must provide that the product shall be the property of the A Corporation, PILP or PW and deemed a work made for hire for copyright purposes unless otherwise approved in writing by an officer of a Related Entity.

**Users Responsibilities**

Responsible Use of Technology

Computing Assets are primarily intended for the business purposes of fulfilling the mission of the A Corporation. Users are responsible to comply with this Policy and to use Computing Assetsin an effective, ethical, and lawful manner. Users may not use Computing Assets for their own personal business or personal benefit, such as using the systems to operate an outside business.

Protection of A Corporation and Related Entities Technology

Prohibitions

Users are prohibited from:

1. using software designed to destroy data, provide unauthorized access to Computing Assets and RE Computing Assets, or disrupt computing processes in any way.
2. introducing into the Computing Assets or RE Computing Assets, intentionally, recklessly or negligently any malware, viruses, worms, Trojan horses, spyware and other invasive and harmful software (collectively “Viruses”). Anti-virus software is installed on all network and computer systems and as a protection for the computer network, as well as any remote Computing Assets accessing the computer network via Citrix.
3. tampering with or modifying anti-virus software or other security software installed and managed by the IT department; Users are required to have it activated at all times.
4. downloading or otherwise introducing into the Computing Assets or RE Computing Assets materials that are protected by copyright or other intellectual property protections.
5. Downloading personal items into the Computing Assets or RE Computing Assets, including, but not limited to, music and movies, which may carry harmful Viruses.

The only exceptions to these prohibitions are items that are downloaded into the Computing Assets or RE Computing Assets for work purposes. However, Users shall not download such items without first consulting with IT and, if necessary, Legal Services.

Passphrases and Passcodes

Users must comply with the password and passcode standards provided by IT, which include the requirement that Users utilize passphrases. Users must maintain passphrases and passcodes on all Computing Assets, including tablets and cell phones. Users are required to maintain the confidentiality of their passphrases. To protect both the A Corporation and the User: (1) Users will not share their passphrases; and (2) Users should not write down their passphrases and leave them where third parties can easily find them.

Users should report immediately to IT any theft or loss of software or Computing Assets or RE Computing Assets used to access the A Corporation’s network.

Upon separation from employment, deployed Users are required to return to IT all Computing Assets, fully intact including contents, as well as any work-related data.

**IT Responsibilities**

Management of Computing Assets

IT is responsible for the complete life cycle management of the Computing Assets, including determining standards, forecasting, planning, funding, ordering, and scheduling replacement of obsolete equipment, and upgrading software and hardware. IT will be responsible for technology evaluation, review, and selection. All technology purchases will be subject to approval by the Director of IT (or a designee within IT).

Installation of Equipment and Software

IT is responsible for the installation of all Computing Assets and RE Computing Assets on the A Corporation network unless IT agrees, in advance, that another qualified party can perform the installation under direct supervision of IT staff. Under no circumstances may a User load onto a Computing Asset, any software or connected peripherals for personal or third-party business purposes.

IT is responsible for installation of all software on A Corporation systemsunless IT agrees in advance that another qualified party can perform the installation. Users are not permitted to install shareware, freeware, open source software, vendor software, demonstration software, or software from the Internet or electronic mail except by advance permission of IT.

Polices for Deployed Staff or Those Who Travel Extensively

Users who travel for extended periods of time or who are deployed regionally may install personal use software on Computing Assets only if: (1) the software is reviewed and approved by IT; (2) the User’s supervisor approves of installation of the software; (3) the software is lawfully acquired by the User for or her personal use; (4) installation of the software does not interfere with or pose a threat to the operation of Computing Assets and the data, documents, and information stored therein; and (5) installation is legally permitted by the software’s license. "Personal Use" software means software not required to carry out functions of assigned job duties. The individual User assumes responsibility for any costs associated with the proper licensing of Personal Use software and for maintaining the license and evidence of payment on file. The A Corporation assumes no liability for copyright violations by the User associated with installations of Personal Use software and reserves the right to require removal of such software at any time. If any violation should occur and an action is brought by a third party against the A Corporation, the User is required to pay the costs of defense (including fees and expenses) and indemnity. If personally installed Personal Use software interferes with any business functions and requires a corrective support call/service, the User and the User’s supervisor will be notified and the software will be promptly removed.

Users deployed regionally or internationally may have agreements with outside vendors and procedures for software installation and maintenance. IT shall be consulted and notified of these agreements and understandings and those Users must comply with all laws regulating the use or export of hardware and software to foreign countries.

Non-Standard and Obsolete Technology

Non-standard and obsolete software and hardware that is currently installed and properly licensed on User systems will continue to receive IT support if that has been the service support arrangement in the past. However, IT may cease supporting software if: (1) the manufacturer no longer provides support, patches, etc. for the Computing Asset; (2) the software is incompatible with A Corporation standard applications, hardware, or operating systems; or (3) if IT is no longer able to support it. IT will notify Users at least six (4) months in advance when any standard software or hardware will no longer be supported as of a specific date. IT also will consult with the affected end Users about replacement options and current budget implications when necessary.

Loaner Pool

IT will provide and maintain a limited pool of computers available for loan to Users for temporary replacement of malfunctioning equipment or for remote use. Request for loaned equipment must be made through the IT Help Desk with the appropriate paperwork completed.

Loaner equipment cannot be deployed for longer than 30 days without approval from the Director of IT (or a designee within IT).

**Standards**

Selection of Standards

IT will be responsible for selecting and ordering the standard technology solutions for the A Corporation and Related Entities. The standards will be reviewed and updated annually.

Criteria for Deployment

Computing Assets will be deployed to support the work of the A Corporation in a cost-effective manner. No more than one computer will be issued to each User unless a request is made by a supervisor or main contact to the IT Help Desk with the appropriate director’s approval.

Replacement Policy

Replacement of desktop machines will occur every five (5) years. Laptops will be replaced every four (4) years. Obsolete equipment that requires excessive support, equipment that is broken, and equipment that cannot provide required performance will be replaced at the discretion of IT.

Retaining hardware and/or software beyond its obsolescence increases the support and maintenance costs for the A Corporation and makes it difficult for Users of the equipment to use current software applications.

Removal of Equipment

IT is responsible for removing and storing equipment, including software and peripherals, when a User is no longer using that equipment or when the equipment reached end of life. The removed equipment of A Corporation will be used for redeployment, sale to staff, donation, will be disposed of, or placed in the IT Loaner Pool. Equipment of Related Entities is returned to that Entity if requested. The equipment should be held for future use in the particular area, a request will be made through the IT Help Desk. All retired and returned equipment that can no longer be supported by IT cannot be connected to the Computing Assets.

The Director of IT or designee (“Director/designee) shall dispose of equipment when it is no longer of use to a User and is discontinued by a supervisor in an A Corporation department or area who does not ask that it be held for future use. If the Director/designee determines that a User’s discontinued equipment is no longer appropriate for redeployment or the Loaner Pool, the Director/designee may offer that equipment for sale to employees of the A Corporation after removing all A Corporation data or personally identifiable information (“PII”). Related Entities that wish to offer their equipment for sale to their employees or employees of other agencies and entities may contact the Director to ask for assistance in selling equipment.

The process will be as follows:

1. The Director/designee will determine that a piece of equipment will not be redeployed or go into the Loaner Pool and is, therefore, not to continue as equipment used and maintained by the A Corporation. Equipment will be inspected for A Corporation data or PII, which will be removed. The Director/designee and IT will follow appropriate policies and procedures to scrub the equipment of all information and data of the organization as well as software licensed to it.
2. If the equipment is from a Related Entity the Director/designee will follow the same process, except that the equipment will be scrubbed and offered for sale and will not be eligible for the loaner pool.
3. The Director/designee will determine a reasonable value for the piece of equipment, which in 2020 is as follows: (a) laptop $100; (b) desktop $50; (c) iPad $50; (d) cell phone $50. The Director will independently established values annually. All checks submitted to pay for equipment shall be made payable to the Presbyterian Church (U.S.A.), A Corporation.
4. The equipment will first be offered for sale to the User from whom it came who can elect to purchase that equipment within 48 hours by delivery of a check to the Administrative Manager of IT.
5. If the User declines to purchase the equipment, the Director/designee will then decide how to dispose of it or whether to donate it and for equipment of Related Entities the Director/designee will discuss next steps with the Related Entity.
6. The Director/designee will discuss disposal of Related Entity equipment with the Related Entity.
7. Proceeds from the sale of equipment will be applied to the budget line of the department or Related Entity which originally purchased it.
8. The Director/designee and IT will update appropriate records to be shared with the A Corp. Finance & Accounting Department, of equipment offered for sale, the purchaser, and payment of the purchase price.

**Acquisition Policies**

Selection of Vendors

IT will purchase all Computing Assets and services.

All A Corporation and Related Entity requests for Computing Assets will be reviewed, approved, and purchased by IT. Related Entities will be charged for the purchase of RE Computing Assets.

Contractors who work with other Related Entities may have other contractual provisions for software acquisition. Any software purchased must comply with IT software standards if the software runs on the network managed by IT. Software must be compatible to A Corporation’s environment.

Customized Software

Customized software may be developed with a third party to satisfy the business or operational requirements of the Related Entities. All such development of software for use on the A Corporation network must be done in consultation with IT.

Available Software

Available software, such as shareware, freeware, and open source, available from the Internet, distributed by vendors, demonstration software, or received by electronic mail may be acquired by Users on behalf of the Related Entities only with prior IT approval, said approval not to be unreasonably withheld. Users are required to consult with IT before acquiring such software, since it may introduce security vulnerabilities to the network. Users will be held responsible for damage to A Corporation’s technology assets caused by installation and operation of harmful software not approved by IT.

**Use of Software**

Policy on Use of Software

All computer software used on Computing Assets must be licensed and used in accordance with the restrictions and requirements specified by the owners/licensors of the software. The unauthorized duplication of copyrighted software or documentation is a violation of the law and is contrary to established standards of conduct for Users and may constitute a breach of contract with the Related Entities. Users who make, acquire, or use unauthorized copies of computer software or documentation may be subject to disciplinary action leading up to termination. The Technology Policy (Section 611) contained in the PMA and ASG Employee Handbooks is incorporated by reference into this document. Users shall not, nor shall they permit anyone else to, download or upload any material onto Computing Assets, photographs, or images from the Internet or any other source determined in A Corporation’s sole judgment to be obscene or pornographic. Downloading illegal materials, such as child pornography, is a violation of policy and will subject Users to discipline up to and including termination of employment. Such conduct is also a criminal offense and the A Corporation will cooperate with law enforcement authorities concerning criminal conduct. Related Entities are encouraged to adopt technology policies similar to those in the PMA and ASG Employee Handbooks.

Audit and Removal of Software

A Corporation reserves the right to audit anything related to the Computing Assets, including the software installed on all computers owned by the A Corporation or attached to its network and to take any action it deems necessary to protect the interests of the A Corporation. IT may work with the internal auditor of the Administrative Services Group, as-needed, on any audit. Related Entities can request audits by having their executive officer contact the President of the A Corporation.

Unlicensed, illegal, unidentified, or unapproved software installed on Computing Assets is subject to removal upon its discovery after consultation between the User, the User’s supervisor, and IT. If the unapproved software belongs to a visitor, guest and/or non-employee, it will be removed immediately without consulting that person. At its option, the A Corporation will give twenty-four (24) hour notice of removal. Removal may occur before a disagreement or dispute is resolved.

Storage of Software Media

The software installation media, serial numbers, and User license agreements must and will be stored in the IT Media Library, behind a locked door to protect against misuse, theft, loss, or accidental damage. All software installation media must be filed in such a manner as to ensure accurate and prompt retrieval by IT personnel

**Data Security Policy**

**Scope**

This Policy applies to all data and information, regardless of the form or the medium in which it is set, and shall apply to such data created, collected or received by, for, or on behalf of the Related Entities. For purposes of this section of the Policy the data described above will hereinafter collectively be referred to as “Data.”

**Classification of Data**

There are levels of Data collection defined below. Each level needs its own level of protection and its own degree of openness and availability.

Confidential Data

The most sensitive Data that is intended strictly for use by certain employees within the Related Entities. This includes Data whose improper use or disclosure could adversely affect the ability of A Related Entity to accomplish its mission as well as any Data requiring protection under various state and federal laws and/or contracts. Confidential Data is disclosed only to authorized persons. Request for access shall be made through the IT Help Desk which will grant access once appropriate approval is obtained.

Controlled Data

Data that needs some level of protection because its unauthorized disclosure could cause damage internally and/or externally to the Related Entities. Controlled Data is disclosed only to authorized persons. Request for access shall be made through the IT Help Desk which will grant access once appropriate approval is obtained.

Public Data

Data that can be shared internally and/or externally with Users. Requests for this access shall be made through the IT Help Desk which will grant access once appropriate approval is obtained.

Data Collected Through the Web Sites of Related Entities

Data collected from the web sites of Related Entities shall be used solely for the intent it was collected. “Personal Data” means name, birth date, e-mail address, mailing address, social security number, and the last four digits of credit card number. To the extent Personal Data is collected from Related Entity web sites, the disclosure of such Personal Data must be made in strict compliance with the Web Privacy Policy.

**Data Responsibilities**

Physical Security

The physical security of all Data produced and stored onsite and storage equipment, including computer hardware and software is the shared responsibility of building security personnel of the Presbyterian Center, IT, and all Users.

When any computer hardware and/or software owned by an entity of the A Corporation is removed from the Presbyterian Center, the responsibility of physical security rests solely with the employee/User. Users should follow the Best Practices contained in the Recommended Best Practices Regarding: Security of Laptops, Portable Electronic Devices, and Electronic Data, which is set forth in the next section of this Policy.

Information Technology Responsibilities Regarding Data

IT is responsible to:

1. Protect and secure Confidential and Controlled Data by using a layered approach, including router, access restrictions and other configurations on individual machines, a firewall and encryption;
2. Preserve the intended purposes of all Data of its Users;
3. Recover Data after a breach or other disaster;
4. Manage Data:
	1. IT works with the Related Entities to share information on technology and data issues;
	2. IT works with Related Entities to secure Data;
	3. IT works with Related Entities to segregate Data when necessary, with the understanding that in some situations it may not be reasonably possible to segregate Data;
	4. Respond to requests from Related Entities and Users to access Data. Such a request must contain sufficient information to show that the person making the request is entitled to receive and review the Data. Access Request forms are available from IT or on CenterNet under the IT tab.
5. Restrict access to Data. IT may restrict access to Data of any Related Entity or User. If a person seeking to access Data wishes to appeal such a restriction decision, the User can appeal to the President of the A Corporation.
6. Work with the President of the A Corporation to enter into contracts for cloud storage and other storage methods for Data.

User, Contractor, Vendor, and Guest Responsibilities

All Users and guests are responsible to comply with this Policy, the policies in the employee handbooks and personnel policies of the Related Entities, and the Ethics Policy, as relevant. Contractors and vendors must also comply with the terms of the contracts with the Related Entities. Any violation of this Policy by employees of the Related Entities may be cause for disciplinary action up to and including termination of employment. Any violation by volunteers of Related Entities may result in termination of the volunteer relationship. Any violation of this Policy by a contractor or vendor will result in termination of contract.

Employees of the Related Entities, volunteers, contractors, and vendors are required to report immediately to IT any theft, loss or compromise of Data or the Computing Assets.

When employment or a contract ends, the contractor or vendor shall remove any Data from any computer or device that is the property of the contractor or vendor.

Supervisor and Human Resources Responsibilities

When an employee is separated from employment with a Related Entity or when a volunteer ends their service or when a contractor’s or vendor’s contractual service ends, the supervisor or employer representative should immediately notify the Human Resources department (“HR”) (for employees, volunteers or vendors) or IT (for contractors). When HR is notified, HR will promptly notify IT and ask that the former employee or volunteer be locked out of all systems to protect the Data on those systems. If IT is notified about a contractor’s end of service, IT will remove access to all systems. IT will then backup the data from the device, emails from the account, and files from the server. The account is then removed from the network.   The supervisor of the separated staff person may ask for a copy of the data and an email alias if needed.

**Best Practices Regarding: Security of Laptops, Portable Electronic Devices, Portable Drives, and Electronic Data**

**Purpose**

The practices in this section of the Policy are designed to protect and secure laptops and other portable devices (ex. cellular telephones, tablets), and drives (i.e. portable hard drives, flash drives) (“Devices”) and the data stored on such Devices, to address risk management issues related to Devices, and to reduce the expenses of replacement costs for Devices.

**Summary of Best Practices**

1. Employees should secure Devices at work by using a lock and cable if it is feasible.

2. Employees should only remove Devices from the Presbyterian Center when needed for work; otherwise employees should access their computer records at home or other off-site locations through CITRIX or other systems.

3. If employees must take Devices from the Presbyterian Center, they should:

a. Never leave the Device unattended.

b. Never leave the Device in a car, but in an emergency, may lock it in a car trunk.

c. Never trust a stranger to watch a Device.

d. When traveling never check in a Device as if it were luggage or with luggage on a flight or train or ship and should keep the Device (in or out of its travel bag) in view, at security and elsewhere, at all times while in airports, train stations, and other travel facilities. Employees should not place a Device on a security belt through a scanner until the employee is ready to walk through security without interference. Devices should not be placed in the trunk of taxis, underneath a bus nor on the luggage rack of taxis or buses.

4. Employees should password protect their Devices and should not share their password with anyone.

5. If employees are permitted to remove confidential information from the Presbyterian Center (ex. personally identifiable information of employees, donors, etc.), the employee should encrypt the information.

6. If a Device is lost or stolen from an employee, the employee should immediately report the theft to law enforcement and the IT Department since some Devices can be remotely disabled or the contents deleted.

7. Devices belonging to employees who are no longer employed by the Related Entities should be delivered to IT to secure the contents; such Devices should never be given to severed employees without conferring with IT.

8. Employees who use cloud storage (Dropbox and OneDrive) should not store files that contain sensitive information such as credit card numbers, Social Security Numbers, etc.

**Best Practices**

Devices at Work

A desktop or laptop is assigned to only one employee. There are cases in which equipment will be shared by multiple employees. All desktop, PC, and laptop information is on file with IT along with the serial number and model number of the laptop.

Employees who receive a Device from a Related Entity are responsible for the physical security of the Device. All Devices and the data and information stored on them are the property of the Related Entity and are **not** the property of any employee. No employee should have any expectation of privacy in any information or data stored on Devices. Employees are responsible for the safety and security of the Devices issued to them and must maintain the privacy, security, and confidentiality of all information and data stored on them. Employees are expected to comply with employer policies concerning confidential information.

Some employees are issued a security cable and lock to secure their laptops in the office or lockable docking stations. Employees must keep the key to the security cable or dock in a safe, but accessible place, so that the laptop can be easily locked or unlocked. Employees with devices which are not capable of receiving a lock should meet with IT to discuss locking the device in their desk or elsewhere in their office. Other Devices should be kept equally secure in the office.

Devices at Home

Employees should only remove their Devices from the Presbyterian Center when required to do so due to work needs. Employees who have access to a personal computer at home or elsewhere can access their electronic files through Citrix, which is a secure system.

Lost and Stolen Devices, Security Breaches

If an employee discovers that a Device has been lost or stolen or if an employee learns that the security of the contents of the hard drive and systems on the Device have been invaded or compromised or that information on a Device has been stolen or secured by a third party, the employee should make a full report of this immediately to law enforcement officials, then promptly to her/his supervisor, the security staff in the Presbyterian Center (if the theft or loss occurs in the Center), Risk Management, and the IT department. The employee should also attempt to obtain a copy of the police report or seek the assistance of the Security Department to obtain it. Certain Devices, such as iPads, can sometimes be accessed by IT remotely and wiped, so it is vital that employees report the theft promptly so if IT can access the Device, it can be wiped before the contents are accessed by thieves or other third parties.

**Wi-Fi and Internet Use Policy**

Wi-Fi at the Presbyterian Center

The A Corporation offers wireless (“Wi-Fi”) access to employees and those who visit the Presbyterian Center. Wi-Fi is free and available to any visitor to the Presbyterian Center (“Guest”) who brings their own properly configured equipment. Usage of the Wi-Fi network is subject to the following terms and conditions.

Terms of Use

Use of the Wi-Fi network constitutes an agreement by the Users and Guests to be bound by the terms of this Policy as well as local, state, and federal law. Failure to comply with the terms of the Policy will lead to loss of network access, suspension of privileges, and, in appropriate circumstances, may lead to criminal prosecution. By connecting to the Wi-Fi network, Users and Guests (whether authorized Users/Guests or not, lawful or unlawful Users/Guests) automatically consent and agree to allow their connection and use to be monitored, intercepted, recorded, read, copied or captured by the A Corporation and its employees and agents

Privacy/No Liability

The A Corporation is not responsible to insure the privacy of information that Guests transfer over the Wi-Fi network. Guests are responsible for the virus and security protection of their equipment and devices. By using the Wi-Fi network, Users and Guests accept that the A Corporation cannot guarantee the security of the service against unlawful access or use.

The A Corporation assumes no responsibility or liability for damage, theft, or loss of a Guest’s equipment, software, data files, data, information, documents, records or other personal property brought into or used at the Presbyterian Center or on the Wi-Fi network. Users and Guests should guard their equipment at all times and keep all equipment and systems and the data and information stored on them safe and secure at all times.

The A Corporation takes no responsibility, and does not accept liability, for any of its User’s or Guest’s computer activities that violate federal law (including copyright infringement), state law, local law or this Policy. Further, the A Corporation does not accept liability for the any occurrences that result from calling law enforcement officials when it appears that any of these laws or policies was or are being broken.

If Guests use the Wi-Fi network to access content or software owned or licensed by others who ask Guests to accept their terms of use, Guests must comply with those terms. By logging on to the Wi-Fi network Guests agree to compensate the A Corporation fully (damages and legal fees) for any claims or legal action made or threatened against the A Corporation by any third party because a Guest used the Wi-Fi network in a way that violated the law or this Policy. The A Corporation will notify Guests of such claims or legal action.

No Technical Assistance

The A Corporation will not provide technical assistance to Guests. However, if a Guest is a guest of the PMA, OGA, ASG or any of the six General Assembly agencies, an elected or appointed member of one of the six agencies or their respective staff members, committee, task force and/or work group members, they are welcome to report problems to the IT Help Desk (ext. 5177) or the security desk in the lobby for assistance.

Internet Usage of Employees of Related Entities

Maintaining the A Corporation’s Computing Assets involves significant costs. The Computing Assets should be used for Related Entities business purposes only. Occasional and very limited or incidental use of the Computing Assets by employees, such as connection to the internet for personal non-business use, is permitted, as long as it does not burden A Corporation’s Computing Assets and systems (“Systems”). Employees of the Related Entities (and volunteers) should have no expectation of privacy in anything that is sent, received or stored in the Computing Assets and System.

Prohibitions for Employees and Volunteers of Related Entities

Employees and volunteers of Related Entities are prohibited from:

1. Downloading protected materials (ex. copyright protected) from or through the A Corporation’s equipment, network, and Systems.

2. Downloading harmful viruses, worms, and other devices or programs that can harm the A Corporation’s Systems.

3. Downloading or otherwise introducing into the Computing Assets and A Corporation Systems materials that are protected by copyright or other intellectual property protections

4. Downloading into or through the A Corporation’s Systems, (whether by file-sharing or any other method or program), movies, DVDs, CDs or any other type of media from the Internet or email or any other source.

5. Downloading into from the A Corporation Systems onto personal thumb drives, hard drives, devices or other personal items any confidential or proprietary documents, information, data, photographs, files or materials of the Related Entities or their employees, vendors, members, donors, customers or clients or that relate or refer to any of its employees, vendors, members, donors, customers or clients or any Personal Data. Employees are prohibited from downloading, taping or collecting such confidential and proprietary information using wearable technology that has video, audio, and recording capabilities.

6. Using the A Corporation’s Systems to knowingly transmit, retrieve or store any communication that: (a) is discriminatory or harassing; (b) appears derogatory, insulting or abusive to any individual or group; (c) is obscene or pornographic; (d) can be seen as defamatory or threatening; (e) reveals the Related Entities confidential information without authorization; (f) reveals Personal Data; or (g) is used for any purpose that is illegal or contrary to the Related Entities policies, rules or interests.

If the A Corporation is notified of such prohibited, improper or illegal conduct or is charged or sued for such improper conduct engaged in by one of its employees, that employee is subject to corrective action up to and including immediate termination of employment and is responsible for any fines, penalties, interest, legal fees, and judgments found or levied against the A Corporation. Other Related Entities are encouraged to implement similar prohibitions and impose similar discipline for violations.

Guest’s Agreements, Limitations, and Disclaimers

It is a Guest’s sole responsibility to protect their information from all risks associated with using the Wi-Fi network, including any damage, loss, or theft that may occur as a result of such use of it. In using free Internet access and accessing the A Corporation’s Wi-Fi system, Guests agree and release, indemnify, and hold harmless, the A Corporation, its officers, elected members, governing bodies, agencies, agents, employees, and affiliates, from any damage that may result in use of the Wi-Fi network.

By logging into the Wi-Fi network Guests agree that they will not use the Wi-Fi network or allow the network to be used:

- in any way which breaks any law (local, state or federal) or the conditions of any license or rights of others, or this Policy;

- to send offensive, harassing, indecent, menacing, threatening, nuisance or hoax e-mails or other electronic communications or to cause annoyance, inconvenience or needless anxiety to any person;

- to send, knowingly receive, upload, download, or use any material which is offensive, abusive, indecent, defamatory, pornographic, obscene or menacing; or

- in any way that the A Corporation reasonably thinks is, or is likely to, adversely affect how we provide the service to Users or any of our Guests, members, employees, agents, associates or third parties.

- to hack into any third party’s computer or other electronic system.

- to introduce any virus, worm, spyware, Trojan horses or other program or code into any computer, computer system, software or disks of the A Corporation or any third party.

- to engage in any activities intended to aid in identity or credit card theft.

- to engage in any activities or access any material involving the sexual exploitation of minors, child pornography, or the luring of children.

- to violate federal copyright laws by making unauthorized copies of copyrighted or licensed software, data or publications.

- to participate in or commit telecommunications fraud.

If the A Corporation reasonably believes that Guests have misused the Wi-Fi network, it may take immediate action to suspend a Guest’s or User’s use of the network without telling the Guest first.

**Exceptions and Conflict Resolution**

Requests for Exceptions

Requests for exceptions to these policies ~~s~~hould be submitted in writing to the Director of IT for review with Legal Services.

Conflict Resolution with IT

The Director of IT, working with the representatives from other Related Entities and/or ministry areas are responsible to resolve conflicts that occur regarding the application or enforcement of these policies and guidelines. If an issue cannot be resolved, the Related Entity(ies) can take up the issue with the President of the Administrative Services Group.

 Procedure Regarding Policy Violations

Any violation of this Policy shall be reported to the Directors of IT and HR who will determine appropriate disciplinary action in consultation Legal Services. Violations by independent contractors will be reported to Legal Services and to the contractor’s contact person

**Review and Revision of Technology Policy/Distribution**

Annually, the Director of IT will convene a committee comprised of one each representative of OGA, PILP, PW, PMA, and the Legal Services Office. This committee will conduct a review of this Policy. A report of the committee’s findings will be submitted to the President of the A Corporation and final revisions will be submitted for approval to the Board of the A Corporation.

This Policy shall be distributed to all Users and to contracting Related Entities through posting on CenterNet. Contracting Related Entities shall receive this Policy and shall sign an acknowledgment of receipt and compliance. Volunteers serving the A Corporation shall sign an acknowledgement of receipt and compliance. This Policy shall be referenced in all Employee Handbooks. Violation of this Policy or the procedures or guidelines to support it by any User may be cause for disciplinary action up to and including in termination of employment or for a vendor the termination of contract.