Adventist Risk Management, Inc.

Cybersecurity

Online Safety Checklist

Organization:	
Date:	
Inspector:	
Title:	

NOTE: *The following list of inspections provides a form for identifying the "basic" cybersecurity items. This list is by no means a complete list of risk control exposures. A "No" response in the following topics may indicate a need for additional safety/risk management measures.*

Administrative

Item	YES	NO	N/A	Description/Recommendation
1. There are written guidelines in place for:				
• protecting data	◯	◯	◯	
• confidentiality of data	◯	◯	◯	
• expectations of privacy	◯	◯	◯	
• monitoring privacy issues	◯	◯	◯	
• limiting data access and use	◯	◯	◯	
• password management and requirements	◯	◯	◯	
• "bring your own device" (BYOD)	◯	◯	◯	
• handling security incidents	◯	◯	◯	
• social media posting and management	◯	◯	◯	
2. The conference or other legal entity has cyber insurance that covers the organization.	◯	◯	◯	
3. There is a process for verifying third parties' security controls that have access to any personal data.	◯	◯	◯	

Inventory

Item	YES	NO	N/A	Description/Recommendation
1. List of all hardware and software used.	◯	◯	◯	
2. All non-essential software has been removed from ministry devices.	◯	◯	◯	
3. Someone is assigned to track all ministry hardware and software annually.	◯	◯	◯	
4. Inventory of all technology assets with the potential to store or process information, regardless if connected to the network or not.	◯	◯	◯	

Users and Password Management

Item	YES	NO	N/A	Description/Recommendation
1. All wireless networks have passwords.	◯	◯	◯	
2. All system default passwords have been changed.	◯	◯	◯	
3. Wireless networks are configured with WPA2 encryption.	◯	◯	◯	
4. Users have been told about their responsibility for password/account protection.	◯	◯	◯	
5. Establishment of separate administrator and operator accounts, permissions, and passwords.	◯	◯	◯	
6. All passwords are unique and meet the minimum 12-character alpha-numeric requirement.	◯	◯	◯	
7. Multi-factor authentication (MFA or 2FA) has been enabled on all accounts, which offers this additional security layer.	◯	◯	◯	
8. User accounts and network/data access have been set up using the rule of least privilege, which grants access to the level necessary to complete approved actions.	◯	◯	◯	
9. Privileged accounts have been reviewed and restricted as necessary.	◯	◯	◯	
10. Individuals with privileged access have signed a user agreement and undergone a background check.	◯	◯	◯	
11. Unused accounts have been deleted.	◯	◯	◯	
12. Shared credentials/accounts have been identified, and there is documentation regarding who has access. (Shared accounts are not recommended.)	◯	◯	◯	
13. Only role-based permissions are implemented where feasible.	◯	◯	◯	

Connectivity

Item	YES	NO	N/A	Description/Recommendation
1. All Internet of Things (IOT) connected devices are on a separate network segment (VLAN or guest network) that do not have access to internal resources.	○	○	○	
2. All vendor access has been removed when not in active use.	○	○	○	
3. All internet access goes through a firewall.	○	○	○	
4. Guest users only have access to a separate wireless network, and guest devices cannot connect to other guest devices over the Guest network.	○	○	○	
5. Guest users are not able to access internal devices.	○	○	○	

Physical Access

Item	YES	NO	N/A	Description/Recommendation
1. There is documentation about who controls access to all equipment locations, including electrical, mechanical, and communication rooms.	○	○	○	
2. There is documentation about how access to equipment locations is obtained, including after-hours access.	○	○	○	
3. Physical security of system components is confirmed as part of the inventory process.	○	○	○	
4. Unauthorized devices, such as personal mobile devices, are restricted from accessing internal networks.	○	○	○	

Awareness

Item	YES	NO	N/A	Description/Recommendation
1. Users have been trained/educated on the risks of installing new software related to the work of the ministry (e.g., games, chat, shopping apps, etc.).	○	○	○	
2. All personnel interacting with ministry computers receive cybersecurity awareness training at least once each year.	○	○	○	
3. Users have signed an agreement not to misuse ministry devices or internet access.	○	○	○	

Process

Item	YES	NO	N/A	Description/Recommendation
1. There is a documented cyber-incident response plan for all devices and systems.	○	○	○	
2. System logs are collected, reviewed, and appropriate actions taken.	○	○	○	
3. All systems are updated automatically, with the latest patches installed on release.	○	○	○	
4. All software is updated automatically, with the latest patches installed on release.	○	○	○	
5. Firewalls are enabled on all devices.	○	○	○	
6. All systems are running antivirus software that is regularly updated.	○	○	○	
7. All systems that can no longer be updated and/or patched are removed from the network.	○	○	○	
8. Offline backups are used and tested at least quarterly.	○	○	○	
9. All portable devices and drives are encrypted.	○	○	○	
10. All connections to the internet are filtered to prevent malware or unwanted content from being accessed on the ministry network or systems.	○	○	○	
11. Unused network data drops are unplugged from the network, so they cannot be used without authorization.	○	○	○	
12. Only approved cloud services are used, and their use is documented	○	○	○	