400 Bring Your Own Device (BYOD) Policy v2

400 BRING YOUR OWN DEVICE (BYOD) POLICY

400.1 Introduction:

This Bring Your Own Device (BYOD) Policy outlines the guidelines and responsibilities for employees, volunteers, contractors, and any individuals who use their personal devices to access the Archdiocese of Baltimore’s network, systems, and data. This policy aims to balance the benefits of BYOD with the need to protect sensitive information and maintain a secure computing environment.

400.2 Purpose:

The purpose of this policy is to establish clear expectations and requirements for the use of personal devices in a maimer that ensures the security, confidentiality, and integrity of the Archdiocese of Baltimore’s data. It also aims to provide guidelines for the protection of personal devices from potential security threats.

400.3 Scope:

This policy applies to all individuals who choose to use their personal devices (including but not limited to smartphones, tablets, laptops) to access the Archdiocese of Baltimore’s resources, whether on-premises or remotely.

400.4 Policy Guidelines:

4.1 . Device Eligibility: Only devices that meet minimum security

requirements and are approved by the IT department may be used for BYOD purposes. The IT department will provide a list of supported devices and operating systems.

4.2. Security Measures: Individuals using personal devices for work-related purposes must ensure the following security measures are implemented:

a. Device Passcode: Devices must be protected with a strong passcode or biometric authentication.

b. Operating System Updates: Devices must have the latest security patches and updates installed.

c. Antivirus and Anti-malware Software: Devices must have up-to-date antivirus and antimalware software installed and regularly updated.

d. Data Encryption: Devices must have data encryption enabled to protect sensitive information in case of loss or theft.

4.3. Access and Authentication: individuals must follow the organization's access and authentication policies when using their personal devices to access the Archdiocese of Baltimore's network or systems. This includes the use of strong, unique passwords, multi-factor authentication where available, and regular password changes.

4.4. Acceptable Use: Individuals must adhere to the Archdiocese of Baltimore's Acceptable Use Policy when using their personal devices for work-related purposes. This includes refraining from accessing or storing inappropriate, offensive. or unauthorized content on their devices.

4.5. Data Protection: Individuals must take appropriate measures to protect the Archdiocese of Baltimore's data when accessed or stored on their personal devices. This includes avoiding unauthorized sharing of data. using secure file storage and sharing methods approved by the organization, and promptly reporting any data breaches or incidents.

4.6. Remote Wipe: Individuals must acknowledge that the Archdiocese of Baltimore reserves the right to remotely wipe data from personal devices used for work purposes in case of loss, theft, or unauthorized access.

4.7. Employee Liability: Individuals are solely responsible for the security and maintenance of their personal devices, including any associated costs.

400.5 Support and Compliance:

5. 1. Device Support: The organization’s IT department will provide limited support for BYOD devices. focusing on network connectivity, access to authorized resources, and assistance with security configurations.

5.2. Compliance Monitoring : The Archdiocese of Baltimore reserves the right to monitor BYOD devices to ensure compliance with this policy and applicable laws. Individuals should have no expectation of privacy when using their personal devices for work-related purposes.

400.6 Policy Acknowledgement:

By using their personal devices for work-related purposes. individuals acknowledge their understanding and acceptance of this BYOD Policy. Failure to comply with this policy may result in disciplinary actions. including the revocation of BYOD privileges and potential legal consequences.

Please note that this is a general example and should be customized to fit the specific needs and requirements of the Catholic organization. It is recommended to seek legal advice and consult with relevant stakeholders when drafting or implementing a BYOD policy.