200 Information Security Policy v2

200 INFORMATION SECURITY POLICY

200.1 Introduction:

This Information Security Policy outlines the guidelines and measures for protecting the confidentiality, integrity, and availability of information assets with in the Archdiocese of Baltimore. This policy applies to all employees, volunteers, contractors, and any individuals granted access to the organization's information systems and data.

200.2 Purpose:

The purpose of this policy is to establish a framework for information security management to ensure the secure handling, storage, and transmission of sensitive information. By adhering to this policy, we aim to protect the organization's reputation, prevent unauthorized access or disclosure, and comply with legal and regulatory requirements.

200.3 Information Classification:

3.1. Classification Levels: Information assets should be classified into appropriate levels (e.g., Public, Internal, Confidential, Highly Confidential) based on their sensitivity, criticality, and potential impact.

3 .2. Handling and Protection: Each classification level requires specific controls and safeguards to ensure proper handling, storage, transmission, and disposal of information assets.

200.4 Access Control:

4.1. User Access Management: Access to information systems, networks, and data should be granted based on the principle of least privilege. Users

should only be given access necessary to perform their job responsibilities.

4.2. User Authentication: Strong authentication mechanisms, such as unique usernames and complex passwords, should be implemented to ensure authorized access and protect against unauthorized use.

4.3 . User Account Management: User accounts should be regularly reviewed, and access rights should be promptly modified or revoked upon changes in job roles or termination of employment.

200.5 Data Protection:

5.1. Data Encryption: Confidential and sensitive data, both at rest and in transit, should be encrypted using approved encryption algorithms and protocols.

5.2. Backup and Recovery: Regular backups of critical data should be performed and tested to ensure data availability in the event of a system failure. data loss, or a security incident.

5.3 . Mobile Device Security: Mobile devices containing sensitive information should be protected with strong passwords, encrypted storage, and remote wipe capabilities. Appropriate security controls should be implemented to mitigate the risks associated with mobile device use.

200.6 Security Awareness and Training:

6.1. Security Awareness: Regular security awareness programs should be conducted to educate employees and other authorized users about their responsibilities. best practices. and emerging threats.

6.2. Training: Employees and authorized users should receive training on specific security topics relevant to their job roles, such as data handling, incident reporting, and incident response procedures.

200.7 Incident Management:

7. I . Incident Reporting: All security incidents and breaches. including suspected or actual unauthorized access, data breaches, or malware infections, must be reported promptly to the designated IT or security personnel.

7.2. Incident Response: An incident response plan should be in place, outlining the steps to be followed in the event of a security incident. The plan should include roles and responsibilities, communication procedures. and procedures for containment, eradication. and recovery.

200.8 Policy Compliance:

8.1 . Compliance Monitoring: Regular monitoring and auditing of systems, networks, and user activities should be conducted to ensure compliance with this policy and detect any violations or security breaches.

8.2. Policy Review: This policy will be reviewed periodically to align with changing technology, emerging threats, and regulatory requirements. Any updates or modifications will be communicated to all employees and authorized users.