900 Employee Training and Awareness Policy v2

900 EMPLOYEE TRAINING AND AWARENESS POLICY

900.1 Purpose:

The purpose of this Employee Training and Awareness Policy is to ensure that all employees of the Archdiocese of Baltimore receive the necessary training and guidance to understand their responsibilities in maintaining a secure and compliant environment. This policy aims to raise awareness of information security best practices, privacy regulations, and ethical conduct in line with the mission and values of the organization.

900.2 Scope:

This policy applies to all employees, volunteers, contractors, and any individuals affiliated with the Archdiocese of Baltimore who handle, access, or process sensitive information or have responsibilities related to information security.

900.3 Training Program:

3.1. Initial Training

a. All new employees and volunteers will receive comprehensive training on information security policies, procedures, and practices during their onboarding process.

b. The initial training will cover topics such as data protection, acceptable use of technology resources, confidentiality requirements, and compliance with relevant laws and regulations.

3.2. Ongoing Training

a. Regular training sessions will be conducted to reinforce information security awareness and promote a culture of privacy and compliance.

b. Training sessions will cover emerging threats, new technologies, changes in regulations, and any relevant updates to policies and procedures.

900.4 Training Topics:

4.1. Information Security

a. Importance of information security and the potential risks associated with data breaches, cyber threats, and unauthorized disclosure.

b. Best practices for creating strong passwords, securing devices, and protecting sensitive information.

c. Recognizing and reporting security incidents, phishing attempts, and suspicious activities.

4.2. Data Protection and Privacy

a. Understanding the organization’s data protection and privacy policies, including the handling of personal and confidential information.

b. Compliance with applicable data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or other local privacy laws.

4.3. Ethical Conduct

a. Upholding ethical standards in the use of technology. handling of information, and interactions with colleagues, clients, and stakeholders.

b. Promoting inclusivity, respect, and professionalism in all communication channels, including email, social media, and other online platforms.

900.5 Recordkeeping:

Records of employee training sessions, attendance. and completion will be maintained to track compliance with training requirements.

900.6 Compliance and Consequences:

Failure to comply with the Employee Training and Awareness Policy may result in disciplinary action, up to and including retraining. suspension, or

termination of employment or volunteer service, depending on the severity and frequency of the violation.

900.7 Policy Review:

This Employee Training and Awareness Policy will be reviewed periodically to ensure its effectiveness, relevance, and compliance with changing social media trends and legal requirements.