600 Incident Response Policy v2

600 INCIDENT RESPONSE POLICY

600.1 Purpose:

The purpose of this Incident Response Pol icy is to establish a structured and coordinated approach to detecting, responding to, and recovering from security incidents within the Archdiocese of Baltimore. The policy aims to minimize the impact of incidents, protect sensitive information, and ensure the continuity of operations.

600.2 Scope:

This policy applies to all employees, volunteers, contractors, and any individuals who have access to the Archdiocese of Baltimore's systems, data. and network resources.

600.3 Incident Response Framework:

3.1. Incident Identification

a. Employees and stakeholders are encouraged to promptly report any suspicious activities, security breaches, or potential incidents to the IT department or designated incident response team.

b. Proactive monitoring systems will be implemented to detect and identify potential security incidents.

3.2. Incident Response Team

a. An incident response team comprising representatives from relevant departments will be established to oversee incident response activities.

b. The incident response team will include members with technical expertise, legal knowledge, and communication skills necessary to effectively respond to incidents.

3 .3. Inc ident Response Plan

a. An incident response plan will be developed, maintained, and regularly reviewed to outline the organization’s procedures, roles, and responsibilities during incident response.
b. The incident response plan will address incident assessment, containment, eradication, recovery, and lessons learned.

3 .4. Incident Classification and Escalation

a. Incidents will be classified based on severity . impact, and potential risks to the organization.
b. An escalation process will be established to ensure appropriate stakeholders are notified based on the severity and nature of the incident.

600.4 Incident Response Procedures:

4.1. Incident Assessment and Containment

a. The incident response team will promptly assess the nature. scope, and impact of the incident.
b. Immediate actions will be taken to contain and isolate the incident to prevent fu1ther damage and unauthorized access.

4.2. Incident Eradication and Recovery

a. Efforts will be made to eradicate the incident, remove any malicious presence, and restore affected systems to a secure state.
b. Data backups and restoration procedures will be implemented to ensure business continuity and minimize data loss.

4.3. Communication and Reporting

a. Clear communication channels will be established to notify relevant stakeholders, including senior management, legal authorities, and affected individuals, as required by applicable laws and regulations.
b. Incident reports will be generated, documenting the incident details. response actions, and lessons learned.

600.5 Training and Awareness:

a. Ongoing training and awareness programs will be conducted to educate employees about their roles and responsibilities in incident repo1ting and response.
b. Employees will be trained on recognizing potential security incidents,

repotting procedures, and incident response best practices.

600.6 Policy Review:

This Incident Response Policy will be reviewed on a periodic basis to ensure its effectiveness and alignment with evolving security threats and industry best practices.

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 an Incident Response Policy.