**Parish Data Security Incident Response Annex**

# Purpose:

This Security Response Annex provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis. Specifically, this Annex provides contact information, escalation paths, expected service level agreements, severity and impact classification, and mitigation/remediation timelines. By requiring incorporation of this Annex as part of their Emergency Operations Plan and business continuity of operations plan, the Diocese ensures that when an incident occurs, swift mitigation and remediation ensues.

# Scope:

This plan applies to all data that resides on the parish network and/or storage devices and cloud storage.

Cyber Security Response Team Contact Information:

**Primary Response Team Members: Secondary Response Team Members:**

|  |  |
| --- | --- |
| **IT Coordinator**  | **Technology Consultant** |
| Office Phone  | Office Phone:  |
| Cellular Phone:  | Cellular Phone:  |
| Email:  | Email:  |
|  |  |
| **Business Manager** | **Office Manager (or staff)** |
| Office Phone:  | Office Phone:  |
| Cellular Phone:  | Home Phone:  |
| Email:  | Email:  |
|  |  |
| **Response Team (Pastor)** | **Response Team** |
| Office Phone:  | Office Phone:  |
| Cellular Phone:  | Cellular Phone:  |
| Email:  | Email:  |
|  |  |
| **Principal** | **Assistant Principal** |
| Office Phone: | Office Phone:  |
| Cellular Phone:  | Cellular Phone:  |
| Email:  | Email:  |

Internet Service Provider:

Company Name

Technical Support:

Contact:

Website Host Provider:

Company Name

Office Phone:

Cellular Phone:

Email:

Legal Counsel: Nyemaster Law Firm

Name Frank Harty

Office Phone: (515) 283-3170

After Hours Phone: (515) 249-1995

Email: FHary@nyemaster.com

Insurance Company:

Catholic Mutual Group

Office Phone: 1-800-228-6108 ext. 2444

After Hours Phone: 1-800-228-6108

Email: reportaclaim@catholicmutual.org

Bank

Contact Name:

Office Phone:

Email:

Concept of Operations:

This plan may be activated at levels determined by the following criteria:

1. #1 Level Incident - High:
	1. Examples: Breach of Personable Identifiable Data; Breach of Credit Card Data, Breach of Banking Data, Breach of HIPAA data
2. #2 Level Incident – Medium:
	1. Examples: Breach of Other Files and Documents stored on Parish servers; Breach of Website; Breach of Social Media Site
3. #3 Level Incident – Low:
	1. Examples: Virus or Email Attack; direct disruption of service Attack

## Activation:

Parish staff should immediately report any suspected or implied breach of security to a member of the Primary Response Team who upon notification, will coordinate with the other members of the Team to determine the severity of the incident and activate the plan at the appropriate level. .

In the event the Primary Incident Response Team Member is unavailable, the Secondary Incident Team Response Member will be contacted.

Procedures:

1. Record Data Breach Details: IT Coordinator will coordinate all documentation surrounding the recording of the breach/incident details.
2. Secure the Premises: The Business Manager will secure the physical premises surrounding the data breach/incident.
3. Stop Additional Data Loss: Using your current technology consultant\company, the Response Team will investigate and stop the breach/incident from continuing to occur. Those actions may include:
	1. Block communications back to the bad I.P.
	2. Try not to alter the compromised system.
		1. Do not remove any unidentified connected devices.
		2. Do not kill processes or remove unwanted programs.
	3. Isolate the compromised system from the network.
	4. Attempt to grab some packet captures of suspicious traffic.
	5. Secure a copy of volatile memory.
	6. Secure a forensic image of the system if applicable.
	7. Preserve all logs associated with the affected system.
	8. Complete a Chain of Custody Form (attached) for all evidence collected.
	9. Document all actions taken concerning the compromised system.
	10. Turn the system over to a detailed forensic analyst if appropriate.
	11. If the incident is bank account/monetary funds related, Business Manager will freeze the affected accounts immediately.
	12. If applicable, the Business Manager will contact Catholic Mutual Group.
	13. If applicable, the Business Manager will contact the affected software companies. (I.E. ParishSOFT, Blackbaud, etc.)
4. Assess Priorities & Risks: IT Coordinator, in conjunction with Technology Consulting Firm, will assess the current status of the incident and make recommendations regarding additional technology interference based on current priorities and current risks. Recommendations will be given to the full Incident Response Team.
	1. Determination will be made as to the severity of the incident/breach.
5. Notification: Identify Legal Obligations – Notify Law Enforcement: The Business Manager will contact legal counsel. Based on legal guidance, the Business Manager will contact Law Enforcement.
6. Reporting: Contact and enlist the services of Forensics Investigators: If legal counsel or law enforcement personnel recommend a Forensics Investigation, the IT Coordinator will enlist these services.
7. Communications: The Business Manager will initiate communications with the Diocese of Des Moines. The Diocese will determine the need for notification of all appropriate Diocese financial and information technology personnel. The procedure for dissemination of information regarding the incident is dependent upon the level of plan activation.
	1. Level 3 Activation: All communication is managed within the parish. All parish personnel and appropriate volunteers are to review the Parish Information Systems Security Best Practices.
	2. Level 2 Activation: The Business Manager will communicate with the Diocese to determine if the incident requires activation of the Diocese Communications Team. If yes, the team will coordinate development of a message for dissemination to the public, school, and the community or media (if necessary) by parish staff.
	3. For a Level 1 Activation, all official communications will be directed to the Diocese Communications Director. Parish staff should be directed to avoid making any formal public statements regarding the incident. Refer all inquiries to the Diocese Communications Director.
8. Interview Individual that discovered the breach and all involved: IT Coordinator will conduct a formal interview, in conjunction with forensic analyst if required.
9. Submit all Documentation to full Incident Response Team to review: IT Coordinator will coordinate this documentation and review.
10. Operational Challenges: In the event that the members of the Parish Response Team are fully enveloped in the incident response, parish staff should maintain staff coverage for critical workload needs.

# Plan Maintenance

The plan will be reviewed annually. Parishes should conduct annual “table talk” scenarios to practice walking through the response process, with this document, to ensure the process is correct and that staff are prepared in the event of a real-life incident. Any exception to this plan must be approved by the Bishop of Diocese of Des Moines. Any requests for omission from this plan must be submitted in written form.

# Related Standards, Policies and Processes:

Data Security Policy

Computer Usage and Security Policy

Continuity of Operations Plan

**Parish Information Systems Security Best Practices**

**Minimum Requirements**

1. Have a data backup program in place and current on all computers
2. Install and activate a firewall on every computer/network.
3. Install, activate & maintain updates of an antivirus/anti-malware program on every computer.
4. Utilize a spam filter application to guard against unwanted, harmful emails.
5. Enact a password requirement policy.
6. Enact a password requirement policy.
7. Follow online banking security guidelines

**Resources**

**Firewall**

Microsoft Security Essentials: <https://support.microsoft.com/en-us/help/14210/security-essentials-download>

Zone Alarm Firewall: <https://www.zonealarm.com/software/firewall/>

Privatefirewall Firewall: <http://www.privacyware.com/>

Fortinet Firewall: <http://www.fortinet.com/>

Comodo Firewall: <http://personalfirewall.comodo.com/>

**Antivirus/Malware Removal**

Webroot antivirus: <https://www.webroot.com/us/en/home/sem/brand>

AVG antivirus: <https://www.avg.com/en-us/>

Norton Antivirus: <http://us.norton.com/>

McAfee Antivirus: <http://www.mcafee.com/us/>

Kaspersky Antivirus: <http://usa.kaspersky.com/>

AVAST Antivirus: <http://www.avast.com/>

Spybot Search & Destroy AntiSpyware:

<https://www.safer-networking.org/compare-spybot-editions/>

Spyware Doctor Antispyware: <https://spyware_doctor.en.downloadastro.com/>

**Spam Filter**

Spam Assassin Email Filter: <http://spamassassin.apache.org/>

Appriver Email Filter: <http://www.appriver.com/>

Email Filter: [www.mailwasher.com](http://www.mailwasher.com)

**Data Backup**

Windows 10 System Image Backup: <https://www.windowscentral.com/how-make-full-backup-windows-10>

Datto Corporate: <https://www.datto.com/file-backup-and-sync>

Carbonite: <https://www.carbonite.com/>

**Password Requirement Policy should include:**

* Enforce password activated screen savers/hibernate
* Enforce password protection (i.e. do not share passwords)
* Enforce password strength requirements
* Enforce password refresh timelines
* Establish a password age policy (how often an old password can be used)

**Follow Online Banking Security Guidelines**

* Utilize a stand-alone computer for any online banking transactions with your financial institution
* Do not access any other internet functions from this computer (including email)
* Follow Internal Control & Separation of Duties guidelines
* Remove overdraft protection from all accounts