BARRY UNIVERSITY

DATA SECURITY INCIDENT RESPONSE PROGRAM

Approved by:	**Executive Committee of the Administration**
Approval by ECA	**10/22/2015**
Policy Effective Date:	**10/22/2015**
Related Policies:	**Comprehensive Emergency Management Plan**
Additional References:	**None**

I. Summary

The Data Security Incident Response Program consists of two programs: 1. the Computer Incident Response Program; and 2. Non-Computer Incident Response Program. It provides the framework for responding to computer-based or non-computer based incidents where personally identifiable information (i.e., social security numbers, driver's licenses, passports, etc.), protected health information (i.e., medical records, health insurance information, etc.) or confidential University information has potentially been exposed, whether inadvertently or intentionally.

II. Basic Framework

A. The basic framework of the Data Security Incident Response Program is as follows:

1. Incident Identified. The type of Incident is identified as computer or non-computer.
2. Incident Response Coordinator is appointed to oversee the incident.
3. Incident Assessment. The incident is assessed for level of severity and level of response.

a. *Level of Severity*. The levels of severity take into consideration: exposure of personal information of University constituents and financial impact to the University; non-tangible losses such as reputation and productivity; the extent the incident has spread and how quickly; and the difficulty in bringing the incident under control.

b. *Level of Response*. The levels of response include escalation to the Privacy and Security Committee, Executive Committee of the Administration and through the President to the Board of Trustees.

4. Incident Response Team. As needed and depending on the assessment, the Incident Response Coordinator involves staff with various areas of expertise such as information technology, legal, risk, human resources, public safety, communications, and ECA representatives. Outside resources may also be called upon such as computer forensics and legal counsel.

III. Basic Methodology

The basic methodology of the Incident Response Program emphasizes:

A. Preparation and prevention. Policies and procedures, oversight through Privacy and Security Committee and active monitoring for new vulnerabilities.
B. Detection/analysis. Staff investigates incidents or abnormal/unusual activities that are observed or reported.
C. Containment. Upon confirmation of an incident, staff makes all efforts to contain the incident and the impact of the incident.
D. Eradication. Staff implements measures to prevent the continuation of the incident.
E. Recovery. Once it is confirmed that the incident has been contained and eradicated, staff works to return the University to normal functioning, for example, by restoring network functioning.
F. Post-Incident Activity. The incident is reviewed to determine any issues identified, any changes that need to be implemented or any recommendations that should be addressed.

IV. Barry University Incident Response Program

The complete Incident Response Program is attached.

Barry University

Division of Information Technology

Data Security Incident Response Program

October 2015

TABLE OF CONTENTS

PART I: COMPUTER INCIDENT RESPONSE PROGRAM

1. INTRODUCTION

This Computer Incident Response Program shall be considered a section of Barry University's Comprehensive Emergency Management Plan.

1.1 Objective

Barry University is committed to safeguarding its information infrastructure and complying with regulations such as the *Health Insurance Portability and Accountability Act* (HIPAA), *Family Educational Rights and Privacy Act* (FERPA)*, Health Information Technology for Economic and Clinical Health* (HITECH) Act, Florida Information Protection Act (FIPA), and other state breach notification laws. Consistent with this stance, Barry University is committed to the development of an effective incident response program.

This Computer Incident Response Program (CIRP) document is intended to serve as a guideline for organizing and directing resources in a methodical manner to address security incidents that might adversely affect Barry University's information assets or personal information of employees, faculty, students, alumni, patients, customers or guests. The program as described in this document is intended to achieve the following objectives:

- Protection of the university's information assets and personal information of employees, faculty, students, alumni, patients, customers or guests and the prevention of any illicit utilization of these assets/personal information in malicious activities carried out by or against other organizations.
- Ongoing compliance with regulatory requirements and organizational standards.
- Establish and empower a centralized entity to handle information security incidents or data privacy incidents.
- Development and implementation of a robust incident response mechanism wherein:
    - the cause of the incident is determined,
    - any immediate impact on university constituents (students, faculty, staff, alumni, patients, customers, guests and other affiliates) is effectively limited,
    - efficient containment is effected to prevent further exploitation and exposure,
    - assessment of the impact is performed with tangible or direct measurements such as *financial losses sustained, impact on University constituents* and intangible or indirect measurements such as *reputation loss perceptions*, and
    - ongoing improvement is initiated via regular updates in policies, procedures and incident response capabilities.

1.2 Scope

This Computer Incident Response Program (CIRP) is a general framework for the implementation of incident response standards, policies and practices.

1.3 Sponsoring Organization / Affiliation

The Executive Committee of the Administration (ECA) at Barry University sponsors and supports the CIRP and all efforts relevant to security incident and data privacy incident response. In furtherance of these efforts, the ECA has created the Privacy and Security Committee which operates by a Charter. . The CIRP shall be reviewed on an ongoing basis; however the period between two reviews shall not exceed one year. Incident response capabilities at Barry University will be discussed periodically at the Privacy and Security Committee and recommendations by the Committee shall be made to the ECA.

An Incident Response Coordinator (IRC) will be appointed to oversee all CIRP efforts at Barry University and at least one alternate to the IRC will be appointed to assume the responsibilities of the IRC in the event that the primary IRC is not available. The IRC will report to the Privacy and Security Committee on the adequacy of the CIRP, and submit for review and approval, recommendations for changes deemed necessary and appropriate.

The report from the IRC to the Privacy and Security Committee will be completed at least once per year and will at minimum address the following issues:

1. The status and adequacy of the CIRP and general compliance status.
2. A full report on any new privacy incident since the last reporting period.
3. A full report on any other critical data privacy incidents since the last reporting period.
4. Training status of employees and officers on the CIRP.
5. Results of testing and audits related to the CIRP.

2. INCIDENT RESPONSE

2.1 Incident Definition and Type of Incidents

For the purpose of Incident Response at Barry University, any or all of the following will be treated as an incident:

- An event related to information systems that involves either a violation of a law or a violation of the university's security policy;
- An event related to information systems that causes significant disruption to Barry University's information assets including any damage or unexpected change to the confidentiality, integrity or availability of the information assets or personal information

of University constituents (employees, faculty, students, alumni, patients, customers, guests, etc);

- An event related to information systems that negatively impacts Barry University's constituents.
- An unauthorized acquisition, access, impermissible use or disclosure of unsecured protected health information.

2.1.1 Security Incident Categories

While it is not practical to name every single type of incident or exploit used for illegal activity or willful misconduct, a general classification of incidents is provided below –

Category	Description	Example(s)
Network Scan/Probe	A discovery technique used by potential attackers to identify open ports on targets any any associated vulnerabilities	Ping sweeps, Port scans, etc.
Denial of Service	A type of attack wherein the authorized use of a network, system or application is prevented/impaired by exhausting resources.	Reflector attacks, Amplifier attacks, Distributed Denial of Service (DDoS) attacks, etc.
Malicious Code	A code-based malicious attack that can infect a single host and even propagate to multiple hosts.	Virus, Worm, Trojan horse, etc.
Unauthorized Access	A condition wherein an individual gains logical/physical access to a network, system, application, data or other resource without permission.	Physical Theft, Bruteforce password attacks, Dictionary attacks, Backdoor, etc.

Category	Description	Example(s)
Stolen or Loss of Physical Asset	A condition wherein an authorized user's physical asset (laptop, tablet, storage device, phone, mobile or other electronic device) is either lost or stolen and no longer in the possession of the authorized user.	Lost laptop, stolen device, etc.
Inappropriate Usage	A condition wherein an individual violates the acceptable computing use policies at Barry University.	Storing unauthorized files on work laptop computers/workstations, physical abuse of resources, etc.
Multiple Components	An incident that involves two or more incidents.	Attacks where more than one transmission mechanisms are involved. (*See note below*).

Table 1: *Security Incident Categories*

Note: To distinguish between ***multiple component*** incidents and the other categories, apply the following guidelines:

- *A virus creates a backdoor* – This fits the ***malicious code*** category, and not the ***unauthorized access*** category, because the malicious code is the only transmission mechanism involved.
- *A virus creates a backdoor, and the backdoor is further used to gain unauthorized access* – This fits the ***multiple component*** category because two transmission mechanisms were involved (i.e. the virus, and the backdoor).

Furthermore, the following incidents may require notification to individuals and/or regulatory agencies under contractual commitments or applicable laws and regulations:

- An individual (student, faculty, staff, contractor, or third-party provider) obtained unauthorized access to non-public information maintained in either paper or electronic form.
- An intruder has broken into a database(s) that contains non-public information on an individual.

- Computer equipment such as a workstation, laptop, CD-ROM, or other electronic media containing non-public information on an individual has been lost or stolen.
- A department or unit did not properly dispose of records containing non-public information on an individual or individuals.
- A third party service provider experienced any of the incidents described above, affecting Barry University's data containing non-public university records or records for which the university was entrusted with custodian responsibilities.

In any of the aforementioned cases, the University will determine whether regulatory agencies, local authorities, impacted individuals or university constituents need to be contacted and the appropriate response to media, customers, employees. students, patients, customers or guests.

Refer to Appendix F -Customer Notification section to see the steps to follow to notify impacted individuals and/or regulatory agencies.

2.2 Incident Response Team (IRT)

In order to maintain an efficient incident response mechanism, incident response personnel will be designated to serve on different teams as needed. Based on the category and severity level of the incident in question, one or more of these teams will be required to perform their designated incident response role. Figure 1, below, depicts the Incident Response Organizational Structure at Barry University.

Figure 1: *Incident Response Organizational Structure*

Team	Primary Contact (include work, home, cell and e-mail)	Secondary Contact (include work, home, cell and e-mail)
Incident Response Coordinator	**Associate Chief Information Officer**	**Information Security Office Coordinator**
ECA Representative(s)	**Vice President for Technology & Chief Information Officer** **Vice President for Business and Finance** **Vice President for Human Resources**	
IT Tactical Response Team	**Director, Network & Telecommunications** **Director, Data Operations Center**	**Senior Network Engineer** **Associate Director, Data Center Operations** **Director, Client Services**

	Associate Director, Client Services **Information Security Office Coordinator** **Business System Analyst**	
External Computer Forensics	**Enterprise Risk Management (ERM)**	**Enterprise Risk Management (ERM)**
Internal Legal Counsel – Risk Manager	**Assistant General Counsel & Risk Manager**	**General Counsel**
External Legal Counselors	**McDonald Hopkins**	**McDonald Hopkins**
Human Resources Department	**Vice President of Human Resources**	**Associate Vice President of Human Resources**
Communications	**Vice President of Institutional Advancement**	**Public Relations Manager**
Public Safety	**Director of Public Safety**	**Director of Investigations & Training**

2.3 IRT Methodology

The Incident Response Team (IRT) at Barry University shall adopt the following steps as part its incident response methodology:

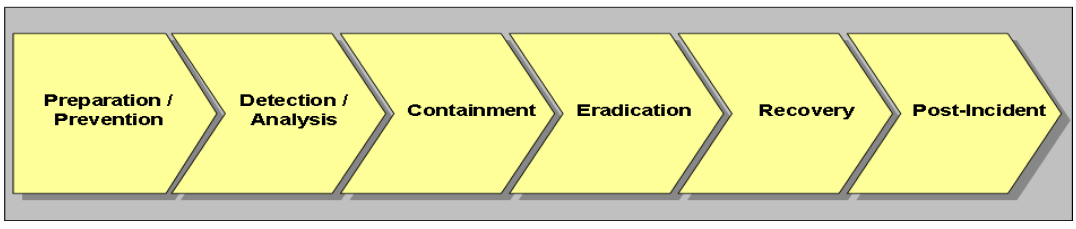

Figure 2: *CIRP Methodology*

Preparation/Prevention

- In keeping with its commitment to robust incident response efforts, Barry University will –
    - Develop policies and procedures to foster efficient and ongoing assessment of risks of IT system related incidents, and to identify and implement countermeasures to mitigate the associated risks to an acceptable level.
    - Maintain the Privacy and Security Committee to oversee incident response efforts as well as define policies and operating procedures.
    - Maintain a contact list of the IRT members with pre-determined points of contact per team.
    - Establish a process whereby active monitoring for new vulnerabilities is performed routinely.
    - Record all activities undertaken when incident response efforts are underway and securely store the recorded information for retrieval at a later date.
    - Modify and adjust the incident response policies and procedures, based on an annual review which will be performed to identify changes in the threat environment along with the associated risks and corresponding countermeasures.
    - Train employees on detecting, reporting, and escalating a potential breach.
    - Test the incident response capability on an ongoing basis, with documented results of each test stored securely for retrieval at a later date.

Detection/Analysis

- The IRT at Barry University will adopt current industry best practices in the detection and analysis of IT system related incidents. The IRT staff shall investigate incidents and/or abnormal activities that are observed or reported. The following best practices will be adopted at a minimum:
    - The Incident Response Coordinator (IRC) will be responsible for managing and coordinating incident response efforts.
    - Documented logs maintained by IRT staff should, when possible, include timestamps.
    - In the event of an incident, the IRT staff is responsible for identifying the extent of the incident and also for identifying the IT systems affected by the incident.
    - Attempts shall be made to identify the type of the incident (e.g. network probe/scan, Virus/Worm attack, Denial of Service etc.) and the source of the incident (e.g. internal, external, third-party, etc.).

- If required, forensic examinations with formal procedures (chain of custody, evidence handling procedures, etc.) shall be carried out either at a host level or a network level or both.
- Based on the type of incident detected, complete the forms included in Appendix A (A.1, A.2, A.3, A.4, A.5, and A.6) accordingly.

Containment

- Upon confirmation of incident(s) the IRT staff at Barry University shall initiate containment efforts in the form of isolation of IT system(s) and/or networked device(s). This may include methods such as manual disconnection from a network(s), logical isolation of a host, etc. In the event that the physical disconnection or logical isolation methods are not possible and/or not helpful, the IRT staff shall isolate the local network to which a system or networked device is attached.
- Keep track of the action and issues taken by completing the forms included in Appendix A (A.7 and A.8).

Eradication

- As a first step in eradication, the IRT staff shall identify and implement measures to prevent the continuation and propagation of an incident. Eradication efforts may include cleaning infected or corrupt files, resetting passwords, and even complete rebuilding of IT systems and/or networked devices that have been affected by an incident, not limited to machine/device compromise alone. Additionally, the IRT staff is also expected to analyze any digital evidence, gathered from forensic efforts or otherwise, to identify the source of the incident and the cause, including the exact vulnerability that was exploited.
- When evaluating the eradication options, consider whether the measures adopted are likely to jeopardize evidence or disrupt the organization services. This may include:
  - Causing damage to or destroying existing evidence;
  - Launching additional attacks upon the organization; or
  - Leaving the organization exposed.
- Keep track of the issues and actions taken by completing the forms included in Appendix A (A.7 and A.8).
- If evidence is acquired complete the Supporting Evidence Inventory form included in the Appendix A (A.9). This form has to be completed in conjunction with the Chain of Custody form included in the evidence handling procedure.

Recovery

- Once eradication efforts have been successfully carried out, the IRT staff will test the affected IT systems and/or networked devices for traces of the vulnerability that was identified as exploited. Once confirmation is obtained regarding the safety of the IT systems and/or networked devices, they shall be reconnected to the network and

restored into the operational function that they initially performed. If necessary, it may be needed to utilize backups for restoration purposes.

- Keep track of the action and issues taken by completing the forms included in Appendix A (A.7 and A.8).

Post-Incident Activity

- After incident response efforts are successfully completed –
  - The IRT staff should create a report of the incident and submit it to the Incident Response Coordinator (IRC). The report should include timestamps when possible, details of each step undertaken during the incident, issues identified, changes implemented, and any further recommendations based on incident understanding.
  - The IRC will present the report to the Privacy and Security Committee for discussion around the need to further identify and assess the larger impact of the incident on the University.
  - The Privacy and Security Committee will give due consideration to the findings and recommendations in the report and initiate actions, with the help of the IRC, to address the recommendations.
  - The Privacy and Security Committee will coordinate efforts with Vice President for Technology & CIO, legal counsel, the IRC and Human Resources to identify whether additional information is required.
  - It is recommended that the Incident Response Coordinator coordinate a lessons learned "post-mortem" with the Incident Response Team staff and/or the Privacy and Security Committee to review the effectiveness of the incident handling process and to identify any necessary improvements to existing security controls and practices.
  - The IRC or assigned IRT member should complete the Post-Incident Evaluation Form included in the Appendix A (A.9) during the lessons learned meeting.

2.4 Incident response and escalation

The incident response protocol at Barry University relies on the use of multiple escalation levels based on the severity level of the incident. In addition to the guidelines provided in Table 2, the following factors must also be taken into consideration when determining the exact escalation level to respond to an incident:

- **Tangible Losses:** Includes any direct and indirect financial damage to Barry University or exposure of personal information of University constituents (employees, faculty, students, alumni, patients, customers, guests or other affiliates).
- **Intangible Losses:** Includes the non-financial aspects of damage such as loss of reputation, image and/or credibility, productivity, etc.

- **Extent:** Includes an assessment of how extensively the incident has spread and how quickly it is propagating.
- **Impact:** Includes an assessment of the difficulty involved in bringing the incident under control.

Level	Teams / Areas Involved	Details	Example(s)
0	1. IT Tactical Response Team	• Regular functioning. • Monitor sources for alerts.	None. This is the default escalation level when there is no incident.
1	1. IT Tactical Response Team 2. IRC	• Threat detected. • Decide on defensive measures to be undertaken.	Network Scan/Probe, Inappropriate Usage.
2	1. IT Tactical Response Team 2. IRC 3. ECA 4. Privacy and Security Committee 5. Human Resources Department 6. External Computer Forensics 7. Internal Legal Counsel/Risk Manager 8. External Legal Counselors 9. Communications	• Threat manifested, and/or damage is underway. • Decide on control, contain and eliminate measures to be undertaken. • Decide on legal measures to be undertaken. • Confidential Information was compromised	Inappropriate Usage, Denial of Service, Malicious Code, Unauthorized Access, Stolen or Loss of Physical Asset, Multiple Components.

Table 2: *Escalation Levels*

2.4.1 Escalation Procedures

Escalation Level 0

A threat or a probable threat has been detected that does not require further escalation.

IT Tactical Response Team

- Monitor sources for alerts of any new and unidentified threat(s).
- Sources include, and are not limited to, those identified in Appendix D: Tools and resources available.

Escalation Level 1

A threat or a probable threat has been detected and requires further escalation.

IT Tactical Response Team

- Decide and implement immediate defensive action to counter the threat.
- Notify the Incident Response Coordinator (IRC).
- Notify employees of any action(s) required from them.
- Track and manage employee notification requests.

Incident Response Coordinator

- Track and manage threats or potential threats reported by the IT Tactical Response Team.
- Notify the Privacy and Security Committee of the possible threat and countermeasures (if any).
- Notify the Privacy and Security Committee if non-public data has been either compromised or suspected to be compromised.
- Escalate the incident to Level 2 if the need is identified.

Escalation Level 2

A threat has manifested itself, and has either begun spreading, inflicting damage or causing the compromise of non-public information.

IT Tactical Response Team

- Decide immediate defensive action to counter, contain and eradicate the threat.
- Implement the measures identified.
- Provide ongoing reports to the Incident Response Coordinator.
- Convene the IRT to discuss whether or not notification is warranted legally.
- Prepare a summary of the IRT recommendation to the Privacy and Security Committee for a final decision on notification.
- If notification is given, track and manage employee notification requests.
- Maintain a detailed logbook of events and activities, including timestamps, whenever possible.
- Notify the Incident Response Coordinator (IRC) to create/update logbook entry activities undertaken regarding any actions taken.

Incident Response Coordinator

- Direct and coordinate the actions of the incident response team and assume complete command of technology tactical efforts during an incident response.
- Notify the Privacy and Security Committee of the threat and any associated damage(s), and also forward ongoing reports received from the IT Tactical Response Team.
- Maintain a detailed logbook of events and activities, including timestamps, whenever possible.
- Notify the Risk Manager, Legal Counsel and Human Resource with specific details of incident severity and implications, if deemed necessary.
- Identify key tasks, manages timelines and documents all response efforts.
- Outline the budget and resources needed to handle the response.

Privacy and Security Committee

- Apprise ECA of incident and ongoing actions and resolution.
- Implement all directives from ECA regarding incident.
- Request legal opinions from internal counsel on requirements under the law.
- Involve the Risk Manager if appropriate.
- Coordinate with the IRC to identify when the risk associated with the incident has been reduced to acceptable levels.
- Determine, in consultation with legal counsel and the IRC the appropriate response to media, customers, and/or employees, and state/federal regulators.
- Manage all communication and coordination efforts with the media.
- Monitor media coverage and circulate accordingly.
- Direct the appropriate Vice President to determine the type and scope of any punitive action if the source of the incident is internal and traced to current students, faculty or staff.

Legal Counsel

- Verify laws and requirements related to the incident.
- Provide Privacy and Security Committee with an opinion on whether or not local authorities need to be contacted.
- Determine with the help of the Privacy and Security Committee, the best course of action to deal with consumer notifications or other related legal requirements (including notice to state/federal regulators).
- Advise on media notification requirements
- Advise on how to handle the incident in case legal action is deemed necessary.

Communications

- Identify communication strategy prior to any incident.
- Control information dissemination regarding the incident.
- Issue press releases or statement to media, as needed and required

- Track and analyze media coverage and quickly respond to any press response during and after a privacy or security incident.

Human Resources

- Work with appropriate employees to correct performance or improve processes or training (if employee performance is a factor in the incident).
- Work with appropriate managers and legal representatives to take appropriate employment action (i.e., termination of employment) and legal action (if employee misconduct is a factor in the incident).

Post-Incident Procedure

The Privacy and Security Committee

- It is recommended that the Privacy and Security Committee perform a post-incident assessment to estimate the extent of damage.
- It is recommended that the Privacy and Security Committee provide a documented update to the ECA and the Board of Trustees with findings from the post-incident assessment along with an executive summary of actions taken, follow-up efforts required post the incident (e.g. updates in policies and procedures, costs involved in any other efforts, etc.), and the actions taken to minimize publicity and liability. The President will communicate with the Board of Trustees.

Incident Response Coordinator

- It is recommended that the Incident Response Coordinator provide a documented report to the Privacy and Security Committee with a complete description of the incident and any recommendations for improvements to the Computer Incident Response Program.
- Provide incident logbook along with system audit logs to the IT Tactical Response Team.
- It is recommended that the Incident Response Coordinator coordinate a lessons learned "post-mortem" meeting with the IRT staff to review how effective the CIRP was and identify necessary improvements to existing security controls and practices.

The escalation procedure to be followed is depicted as a flowchart below:

Escalation procedure Level 0 and Level 1 - Flowchart

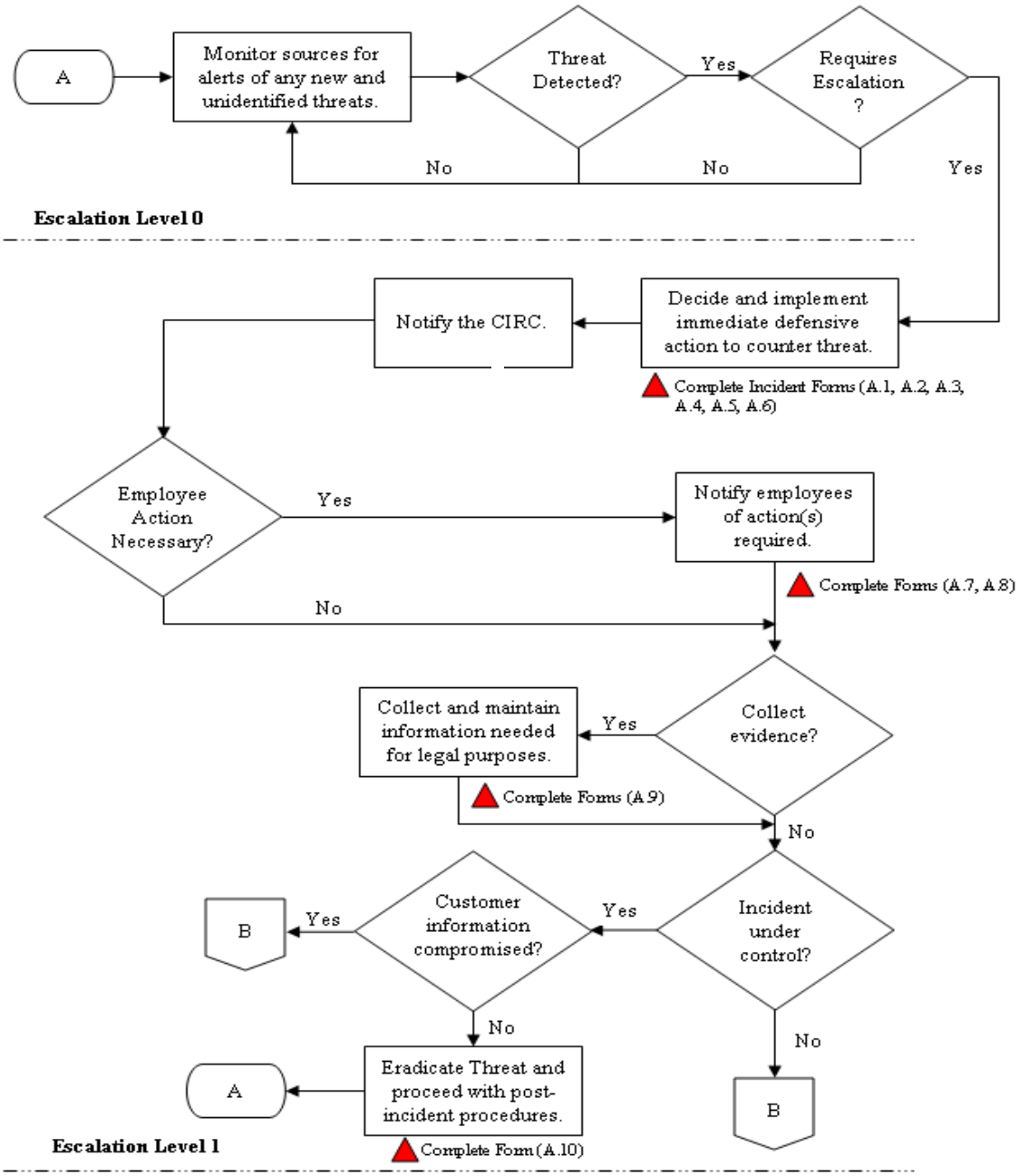

Figure 3: *Escalation Flowchart – Level 0 and Level 1*

Escalation procedure Level 2 - Flowchart

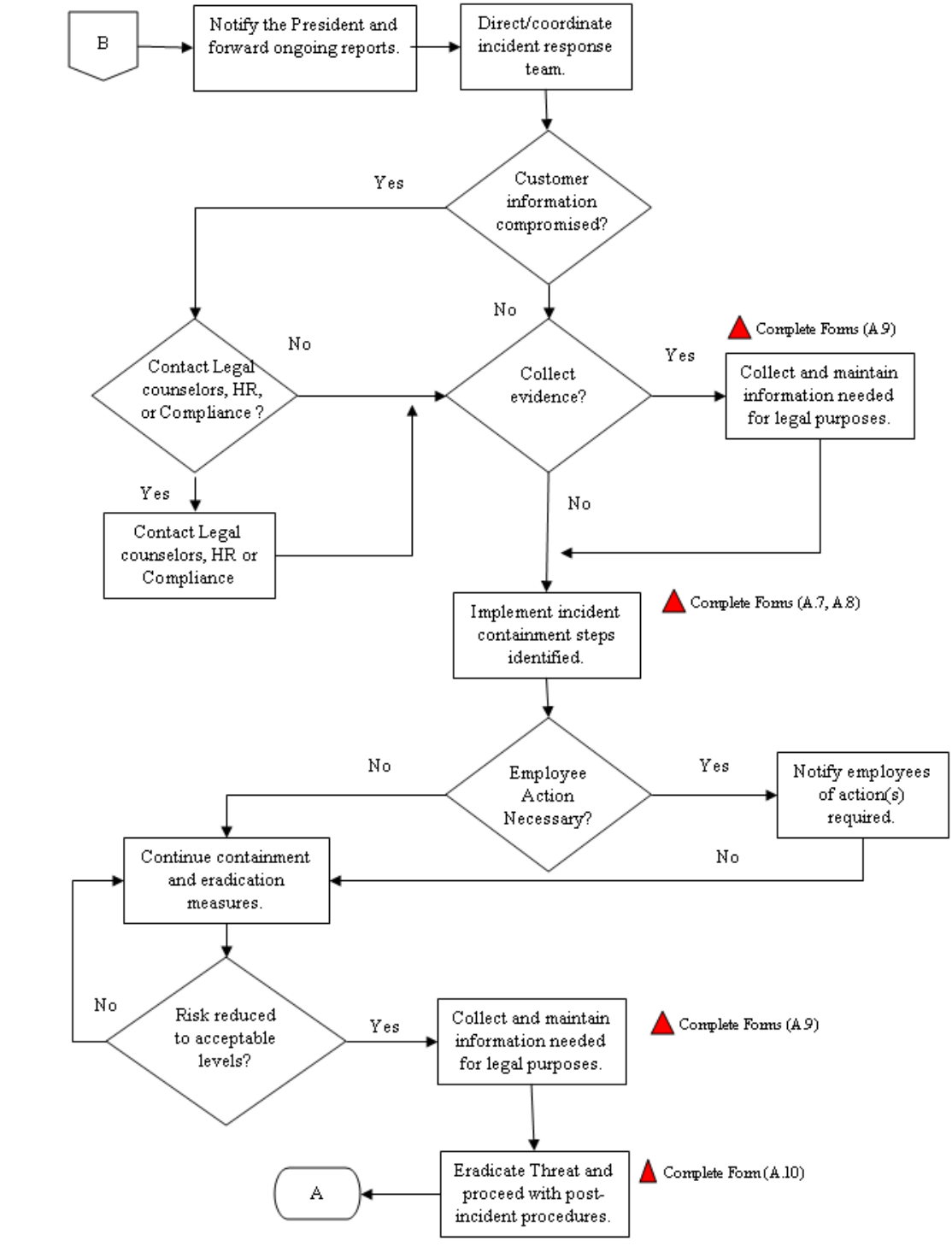

Figure 4: *Escalation Flowchart – Level 2*

3. Sharing information with outside parties

From time to time, Barry University may have incidents that require communication with outside parties. Barry University may report incidents to the United States Computer Emergency Response Team (US-CERT). Additionally, Barry University may choose to communicate with the CERT® Coordination Center (CERT®/CC), law enforcement and media entities.

Depending upon the nature of the incident, Barry University may need to communicate/coordinate with other entities, such as the Internet Service Provider (ISP), service providers and vendor(s), of software deemed as having vulnerabilities during containment/eradication efforts, etc.

The University's external media relations department will be updated along with members of the IRT on the guidelines established for the communication plan. Additionally, all electronic communication with outside parties shall be documented, with timestamps if possible, and stored.

The media relations staff will be established as the only media points of contact (POC) for handling incident communication and related aspects with the media.

4. Legal Counsel

The internal legal counsel and/or designated Risk Manager, will be responsible for the following:

- Working with external legal counsel specializing in incident response and breach management
- Fully understand potential jurisdictional issues (e.g. if a server is located in a state other than that of the main operational workplace and is attacked from a third state).
- Identify and manage any jurisdictional conflicts in the incident reporting process (Note: organizations typically should not report incidents to multiple agencies within the same jurisdiction as this might result in jurisdictional conflicts).

5. Public Safety

The University's Public Safety Department will be responsible for the following:

- Be well acquainted with various law enforcement representatives and fully understand how an incident is to be reported, how the reporting is to be performed, what evidence is to be collected, and how the evidence is to be collected.

- Contact law enforcement via a designated point of contact, following the outlined protocol laid down by law enforcement.

6. Law Enforcement

Barry University, may report incidents and related information to law enforcement authorities. These may include Federal investigatory agencies, such as the Federal Bureau of Investigation (FBI), U. S. Secret Service, etc., district attorney offices and state law enforcement. Appendix E: Security Incident-Related Contacts outlines further contact details of the mentioned agencies and offices.

7. Incident Documentation

The incident response efforts at Barry University requires detailed documentation before, during and after the actual incident(s). All factual data relevant to an incident shall be recorded with timestamps whenever possible. Recorded data shall include all steps undertaken from the point of detection of the incident(s) to the final point of resolution.

The recorded data shall be then stored such that it can be retrieved at a later date. Access to the stored data shall be restricted. Any communication of this data over an electronic medium shall utilize encryption.

Appendix A includes all the basic forms to be used during an incident investigation. The Incident Reporting form (A.1) is a generic form that is to be completed for an incident, regardless of category. Moreover, one specific form is to be filled out (A.2, A.3, A.4, A.5, or A.6) depending on the type of incident. For example, if a virus was reported, the Malicious Code Reporting Form (A.2) is to be filled out. In case of a multiple component incident category, the IRT members should determine the most appropriate forms to fill out.

As the investigation is carried out, additional forms are to be completed. For every action or issue detected during the investigation an Action Form (A.8) is to be filled out and the Action Tracking Log is to be completed.

It is common during an incident investigation that supporting evidence is acquired. Every time new evidence is acquired, it must be inventoried in the Supporting Evidence Inventory (A.9).

Finally, if a lessons learned “post mortem” is conducted the IRC, the Post-Incident Evaluation Form should be completed, detailing how effective the incident handling process was and identifying necessary improvements to existing security controls and practices.

The following chart summarizes the relationship between the forms:

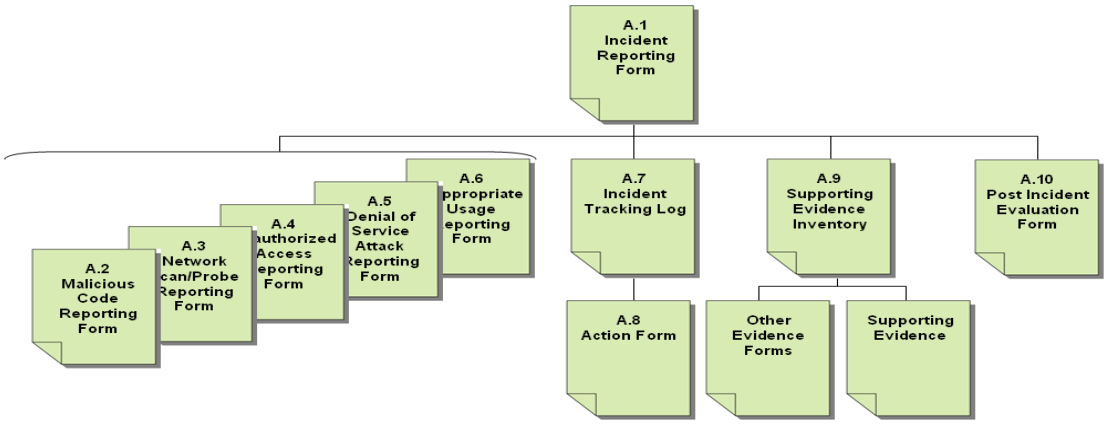

Figure 6: Relationship between Forms

8. Metrics for incident-related data

To bolster ongoing improvements in incident response capability, Barry University should consider translating all post-incident documentation into metrics to measure incident response efficiency. The following metrics should be taken into consideration:

- **Time Per Incident:** Time per incident should be measured to take into consideration the total amount of man-power resources expended on the incident, the total time from the start of the incident to its final resolution, time-lag taken for the incident response team to respond to the incident after the first alarm was raised, and the amount of time taken to coordinate with external agencies.
- **Objective Assessment:** An objective assessment should include review of logs, reports and other post-incident documentation to evaluate how well the corporate incident response policies and procedures were adhered to. This should also include an assessment of how well the incident was documented, whether the incident was detected before the damage commenced, and whether the cause of the incident was identified.
- **Subjective Assessment:** Peer reviews should be conducted after each incident as a means to evaluate incident team member performance. This should include performance before, during and after the incident(s).

Periodic audits should be conducted and should include this Computer Incident Response Program (CIRP), incident response policies and procedures, incident response team training reports, and incident response test documentation/results. The audit should also take into account the metrics defined in this section as well as incident relevant documentation and reports.

PART II: INCIDENT RESPONSE PROGRAM FOR ALL OTHER INCIDENTS (NON-COMPUTER)

1. INTRODUCTION

This Incident Response Program For All Other Incidents (Non-Computer) shall be considered a section of Barry University's Comprehensive Emergency Management Plan.

1.2 Objective

Barry University is committed to safeguarding its information infrastructure and complying with regulations such as the *Health Insurance Portability and Accountability Act* (HIPAA), *Family Educational Rights and Privacy Act* (FERPA)*, Health Information Technology for Economic and Clinical Health* (HITECH) Act, Florida Information Protection Act (FIPA), and other state breach notification laws. Consistent with this stance, Barry University is committed to the development of an effective incident response program.

This Incident Response Program for All Other Incidents (non-Computer) is intended to serve as a guideline for organizing and directing resources in a methodical manner to address security incidents that might adversely affect Barry University's information assets or personal information of employees, faculty, students, alumni, patients, customers or guests. The program as described in this document is intended to achieve the following objectives:

- Protection of the university's information assets and personal information of employees, faculty, students, alumni, patients, customers or guests and the prevention of any illicit utilization of these assets/personal information in malicious activities carried out against other organizations.
- Ongoing compliance with regulatory requirements and organizational standards.
- Establish and empower a centralized entity to handle information security incidents or data privacy incidents.
- Development and implementation of a robust incident response mechanism wherein:
    - the cause of the incident is determined,
    - any immediate impact on university constituents (students, faculty, staff, alumni, patients, customers, guests and other affiliates) is effectively limited,
    - efficient containment is effected to prevent further exploitation and exposure,
    - assessment of the impact is performed with tangible or direct measurements such as *financial losses sustained, impact on University constituents* and intangible or indirect measurements such as *reputation loss perceptions*, and
    - ongoing improvement is initiated via regular updates in policies, procedures and incident response capabilities.

1.2 Scope

This Incident Response Program for All Other Incidents (non-Computer) is a general framework for the implementation of incident response standards, policies and practices.

1.3 Sponsoring Organization / Affiliation

The Executive Committee of the Administration (ECA) at Barry University sponsors and supports the Incident Response Program for All Other Incidents (non-Computer) and all efforts relevant to security incidents and data privacy incident response. In furtherance of these efforts, the ECA has created the Privacy and Security Committee which operates by a Charter. . The Incident Response Program for All Other Incidents (non-Computer) shall be reviewed on an ongoing basis; however the period between two reviews shall not exceed one year. Incident response capabilities at Barry University will be discussed periodically at the Privacy and Security Committee and recommendations by the Committee shall be made to the ECA.

An Incident Response Coordinator (IRC) will be appointed to oversee all Incident Response Program for All Other Incidents (non-Computer) for efforts at Barry University and at least one alternate to the IRC will be appointed to assume the responsibilities of the IRC in the event that the primary IRC is not available. The IRC will report to the Privacy and Security Committee on the adequacy of the Incident Response Program for All Other Incidents (non-Computer), and submit for review and approval, recommendations for changes deemed necessary and appropriate.

The report from the IRC to the Privacy and Security Committee will be completed at least once per year and will at minimum address the following issues:

1. The status and adequacy of the Incident Response Program for All Other Incidents (non-Computer), and general compliance status.
2. A full report on any new privacy incident since the last reporting period.
3. A full report on any other critical data privacy incidents since the last reporting period.
4. Training status of employees and officers on the Incident Response Program for All Other Incidents (non-Computer).
5. Results of testing and audits related to the Incident Response Program for All Other Incidents (non-Computer).

2. INCIDENT RESPONSE

2.1 Incident Definition and Type of Incidents

For the purpose of Incident Response at Barry University, any or all of the following will be treated as an incident:

- An event that involves either a violation of a law or a violation of the University's security policy;
- An event related to information systems that causes significant disruption to Barry University's information assets including any damage or unexpected change to the confidentiality, integrity or availability of the information assets or personal information of University constituents (employees, faculty, students, alumni, patients, customers, guests, etc);
- An event related to information systems that negatively impacts Barry University's constituents.
- An unauthorized acquisition, access, impermissible use or disclosure of unsecured protected health information.

2.1.1 Security Incident Categories

While it is not practical to name every single type of incident or exploit used for illegal activity or willful misconduct, a general classification of incidents is provided below –

Category	Description	Example(s)
Hard Copy Paper	Unauthorized access or impermissible use or disclosure of paper record	Lost or Stolen Paper Record, unauthorized removal of records from secure or other location, improper storage of records
Unauthorized Access	A condition wherein an individual gains physical access to data or other resources without permission.	Physical Theft
Inappropriate Usage	A condition wherein an individual violates the acceptable use policies at Barry University.	Storing unauthorized files, outside of workplace, removing files from workplace, physical abuse of resources, etc.

Table 1: *Security Incident Categories*

The following incidents may require notification to individuals and/or regulatory agencies under contractual commitments or applicable laws and regulations:

- An individual (student, faculty, staff, contractor, or third-party provider) obtained unauthorized access to non-public information maintained in paper form.
- A department or unit did not properly dispose of records containing non-public information on an individual or individuals.
- A third party service provider experienced any of the incidents described above, affecting Barry University's data containing non-public university records or records for which the university was entrusted with custodian responsibilities.

In any of the aforementioned cases, the University will determine whether regulatory agencies, local authorities, impacted individuals or university constituents need to be contacted and the appropriate response to media, customers, employees, students, patients or guests.

Refer to Appendix F -Customer Notification section to see the steps to follow to notify impacted individuals and/or regulatory agencies.

2.2 Incident Response Team (IRT)

In order to maintain an efficient incident response mechanism, incident response personnel will be designated to serve on different teams as needed. Based on the category and severity level of the incident in question, one or more of these teams will be required to perform their designated incident response role. Figure 1, below, depicts the Incident Response Organizational Structure at Barry University.

Figure 1: *Incident Response Organizational Structure*

Team	Primary Contact (include work, home, cell and e-mail)	Secondary Contact (include work, home, cell and e-mail)
Incident Response Coordinator (IRC)	**Associate Vice President for Human Resources**	**Manager, Talent Management**

ECA Representative(s)	**Vice President for Technology** **Vice President for Business and Finance** **Vice President for Human Resources**	
Internal Legal Counsel – Risk Manager	**Associate General Counsel & Risk Manager**	**General Counsel**
External Legal Counselors	**McDonald Hopkins**	**McDonald Hopkins**
Human Resources Department	**Vice President for Human Resources**	**Associate Vice President for Human Resources**
Communications	**Vice President for Institutional Advancement**	**Public Relations Manager**
Public Safety	**Director of Public Safety**	**Director of Investigations & Training**

2.3 IRT Methodology

The Incident Response Team (IRT) at Barry University shall adopt the following steps as part its incident response methodology:

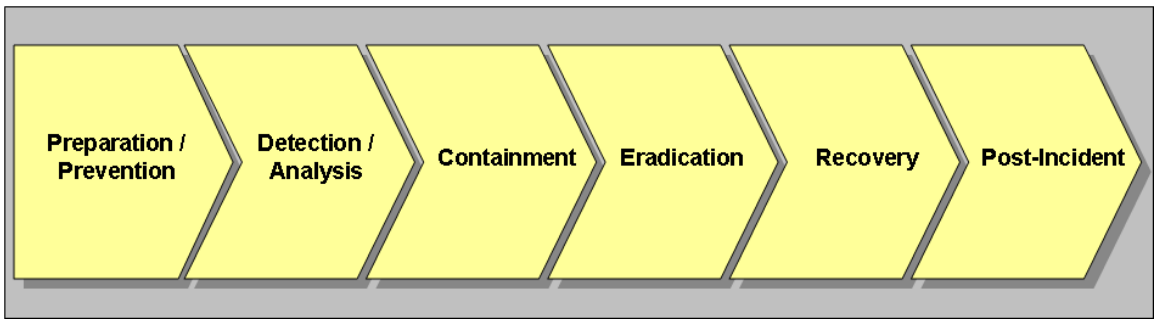

Figure 2: *CIRP Methodology*

Preparation/Prevention

- In keeping with its commitment to robust incident response efforts, Barry University will –
  - Develop policies and procedures to foster efficient and ongoing assessment of risks of incidents, and to identify and implement countermeasures to mitigate the associated risks to an acceptable level.

- Maintain the Privacy and Security Committee to oversee incident response efforts as well as define policies and operating procedures.
- Maintain a contact list of the IRT members.
- Modify and adjust the incident response policies and procedures as needed.
- Train employees on detecting, reporting, and escalating a potential breach.

Detection/Analysis

- The IRT staff shall investigate incidents and/or abnormal activities that are observed or reported. The following best practices will be adopted at a minimum:
  - The Incident Response Coordinator (IRC) will be responsible for managing and coordinating incident response efforts.
  - In the event of an incident, the IRT staff is responsible for identifying the extent of the incident.
  - Attempts shall be made to identify the type of the incident e.g. impermissible access, disclosure, theft, etc.) and the source of the incident (e.g. internal, external, third-party, etc.).
  - If required, forensic examinations with formal procedures (chain of custody, evidence handling procedures, etc.) shall be carried out.
  - Based on the type of incident detected, complete the forms included in Appendix A (A.1, A.2, A.3, A.4, A.5, and A.6) accordingly.

Containment

- Upon confirmation of incident(s) the IRT staff at Barry University shall initiate containment efforts.
- Keep track of the action and issues taken by completing the forms included in Appendix A (A.7 and A.8).

Eradication

- As a first step in eradication, the IRT staff shall identify and implement measures to prevent the continuation and propagation of an incident. Eradication efforts may include removing certain employees access to certain University records.
- When evaluating the eradication options, consider whether the measures adopted are likely to jeopardize evidence or disrupt the organization services. This may include:
  - Causing damage to or destroying existing evidence;
  - Launching additional attacks upon the organization; or
  - Leaving the organization exposed.
- Keep track of the issues and actions taken by completing the forms included in Appendix A (A.7 and A.8).

- If evidence is acquired complete the Supporting Evidence Inventory form included in the Appendix A (A.9). This form has to be completed in conjunction with the Chain of Custody form included in the evidence handling procedure.

Recovery

- All efforts shall be made to recover and preserve University records.
- Keep track of the action and issues taken by completing the forms included in Appendix A (A.7 and A.8).

Post-Incident Activity

- After incident response efforts are successfully completed –
    - The IRT staff shall create a report of the incident and submit it to the Incident Response Coordinator (IRC). The report shall include, details of each step undertaken during the incident, issues identified, changes implemented, and any further recommendations based on incident understanding.
    - The IRC will present the report to the Privacy and Security Committee for discussion around the need to further identify and assess the larger impact of the incident on the university.
    - The Privacy and Security Committee will give due consideration to the findings and recommendations in the report and initiate actions, with the help of the IRC, to address the recommendations.
    - The Privacy and Security Committee will coordinate efforts with Vice President of Information Technology/CIO, legal counsel, the IRC and Human Resources to identify whether additional information is required.
    - It is recommended that the Incident Response Coordinator coordinate a lessons learned "post-mortem" with the Incident Response Team staff and/or the Privacy and Security Committee to review the effectiveness of the incident handling process and to identify any necessary improvements to existing security controls and practices.
    - The IRC or assigned IRT member should complete the Post-Incident Evaluation Form included in the Appendix A (A.9) during the lessons learned meeting.

2.4 Incident response and escalation

The incident response protocol at Barry University relies on the use of multiple escalation levels based on the severity level of the incident. In addition to the guidelines provided in Table 2, the following factors must also be taken into consideration when determining the exact escalation level to respond to an incident:

- **Tangible Losses:** Includes any direct and indirect financial damage to Barry University or exposure of personal information of University constituents (employees, faculty, students, alumni, patients, customers, guests or other affiliates).
- **Intangible Losses:** Includes the non-financial aspects of damage such as loss of reputation, image and/or credibility, productivity, etc.
- **Extent:** Includes an assessment of how extensively the incident has spread and how quickly it is propagating.
- **Impact:** Includes an assessment of the difficulty involved in bringing the incident under control.

Level	Teams / Areas Involved	Details	Example(s)
0		• Regular functioning. • Monitor sources for alerts.	None. This is the default escalation level when there is no incident.
1	1. IRC	• Threat detected. • Decide on defensive measures to be undertaken.	Unauthorized Usage of Paper Records.
2	1. IRC 2. Privacy and Security Committee 3. Human Resources Department 4. Internal Legal Counsel/Risk Manager 5. External Legal Counselors 6.Communications	• Threat manifested, and/or damage is underway. • Decide on control, contain and eliminate measures to be undertaken. • Decide on legal measures to be undertaken. • Confidential Information was compromised	Inappropriate Usage, Unauthorized Access, Stolen or Loss of Physical Asset, Multiple Components.

Table 2: *Escalation Levels*

2.4.1 Escalation Procedures

Escalation Level 0

A threat or a probable threat has been detected that does not require further escalation.

- Monitor sources for alerts of any new and unidentified threat(s).

- Sources include, and are not limited to, those identified in Appendix D: Tools and resources available.

Escalation Level 1

A threat or a probable threat has been detected and requires further escalation.

Incident Response Coordinator

- Track and manage threats or potential threats reported or noticed.
- Notify the Privacy and Security Committee of the possible threat and countermeasures (if any).
- Notify the Privacy and Security Committee if non-public data has been either compromised or suspected to be compromised.
- Escalate the incident to Level 2 if the need is identified.

Escalation Level 2

A threat has manifested itself, which has inflicted damage or has caused the compromise of non-public information.

Incident Response Team

- Decide immediate defensive action to counter, contain and eradicate the threat.
- Implement the measures identified.
- Provide ongoing reports to the Incident Response Coordinator.
- Convene the IRT to discuss whether or not notification is warranted legally.
- Prepare a summary of the IRT recommendation to the Privacy and Security Committee for a final decision on notification.
- If notification is given, track and manage employee notification requests.

Incident Response Coordinator

- Direct and coordinate the actions of the incident response team and assume complete command of efforts during an incident response.
- Notify the Privacy and Security Committee of the threat and any associated damage(s), and also forward ongoing reports received from the incident response team.
- Notify the Risk Manager, Legal Counsel and Human Resource with specific details of incident severity and implications, if deemed necessary
- Identify key tasks, manages timelines and documents all response efforts

Privacy and Security Committee

- Apprise ECA of incident and ongoing actions and resolution.
- Implement all directives from ECA regarding incident.

- Request legal opinions from internal counsel on requirements under the law.
- Consult with Risk Manager.
- Coordinate with the IRC to identify when the risk associated with the incident has been reduced to acceptable levels.
- Determine, in consultation with legal counsel and the IRC the appropriate response to media, customers, and/or employees, and state/federal regulators.
- Manage all communication and coordination efforts with the media.
- Monitor media coverage and circulate accordingly.
- Direct the appropriate Vice President to determine the type and scope of any punitive action if the source of the incident is internal and traced to current students, faculty or staff.

Legal Counsel

- Verify laws and requirements related to the incident.
- Provide Privacy and Security Committee with an opinion on whether or not local authorities need to be contacted.
- Determine with the help of the Privacy and Security Committee, the best course of action to deal with consumer notifications or other related legal requirements (including notice to state/federal regulators).
- Advise on media notification requirements
- Advise on how to handle the incident in case legal action is deemed necessary.

Communications

- Identify communication strategy prior to any incident.
- Control information dissemination regarding the incident.
- Issue press releases or statement to media, as needed and required.
- Track and analyze media coverage and quickly respond to any press response during and after a privacy or security incident.

Human Resource

- Work with appropriate employees to correct performance or improve processes or training (if employee performance is a factor in the incident).
- Work with appropriate managers and legal representatives to take appropriate employment action (i.e., termination of employment) and legal action (if employee misconduct is a factor in the incident).

Post-Incident Procedure

The Privacy and Security Committee

- It is recommended that the Privacy and Security Committee perform a post-incident assessment to estimate the extent of damage.
- It is recommended that the Privacy and Security Committee provide a documented update to the ECA and the Board of Trustees with findings from the post-incident assessment along with an executive summary of actions taken, follow-up efforts required post the incident (e.g. updates in policies and procedures, costs involved in any other efforts, etc.), and the actions taken to minimize publicity and liability. The President will communicate with the Board of Trustees.

Incident Response Coordinator

- It is recommended that the Incident Response Coordinator provide a documented report to the Privacy and Security Committee with a complete description of the incident and any recommendations for improvements to the Computer Incident Response Program.
- It is recommended that the Incident Response Coordinator coordinate a lessons learned "post-mortem" meeting with the IRT staff to review how effective the Incident Response Program for All Other Incidents (non-Computer) was and identify necessary improvements to existing security controls and practices.

The escalation procedure to be followed is depicted as a flowchart below:

Escalation procedure Level 0 and Level 1 - Flowchart

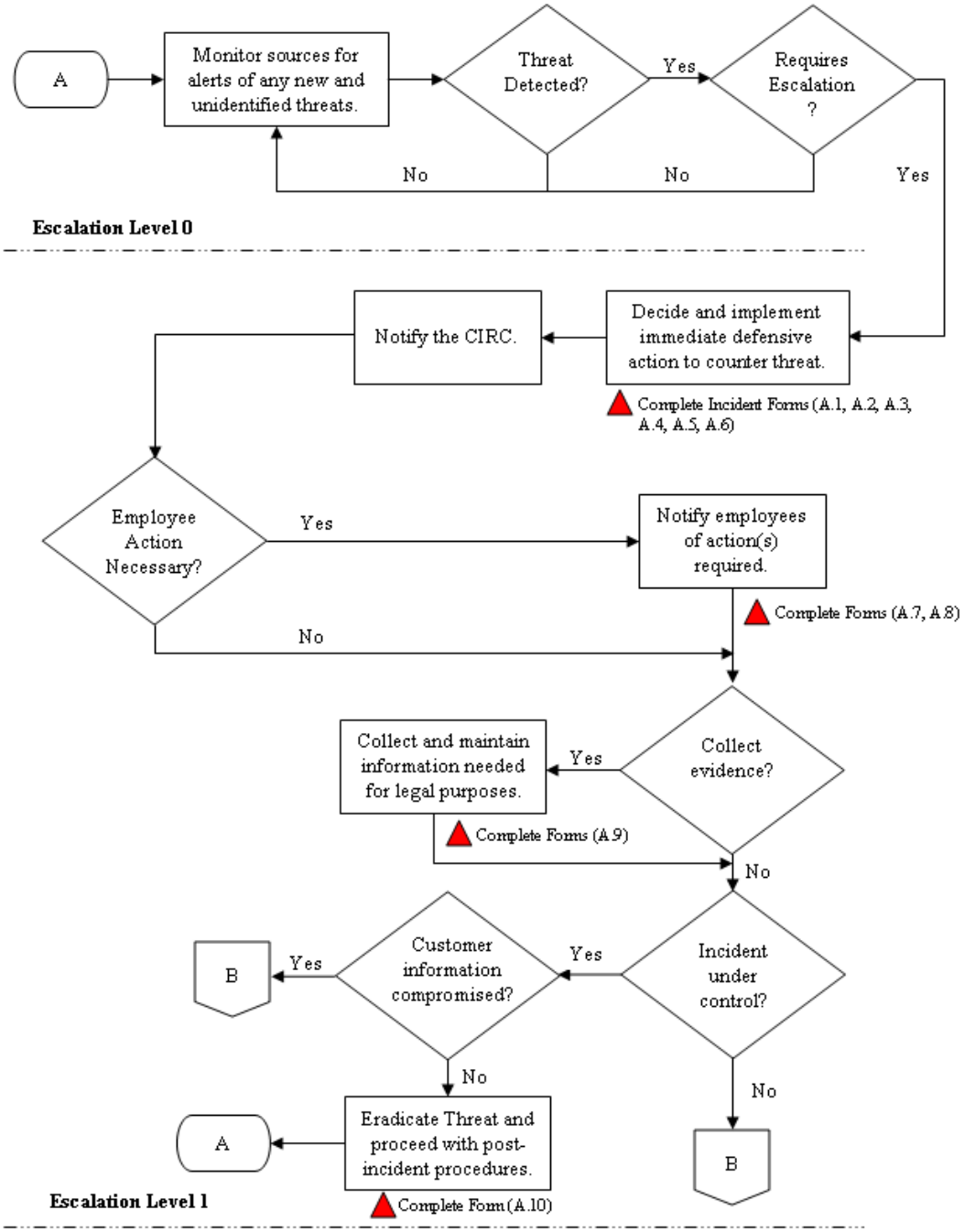

Figure 3: *Escalation Flowchart – Level 0 and Level 1*

Escalation procedure Level 2 - Flowchart

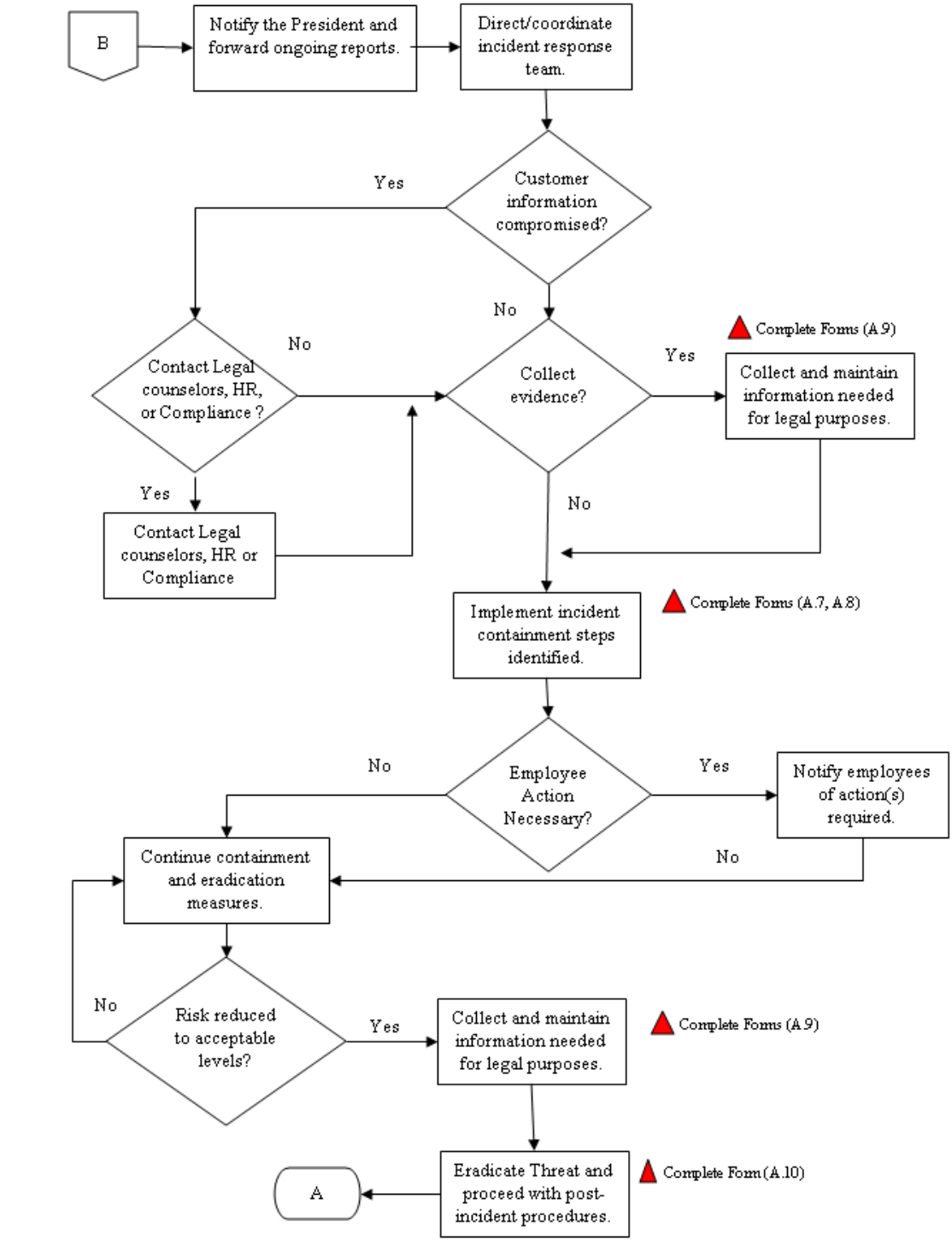

Figure 4: *Escalation Flowchart – Level 2*

3. Sharing information with outside parties

From time to time, Barry University may have incidents that require communication with outside parties. Barry University may report incidents to the United States Computer Emergency Response Team (US-CERT). Additionally, Barry University may choose to communicate with the CERT® Coordination Center (CERT®/CC), law enforcement and media entities.

Depending upon the nature of the incident, Barry University may need to communicate/coordinate with other entities, such as the Internet Service Provider (ISP), service providers and vendor(s), of software deemed as having vulnerabilities during containment/eradication efforts, etc.

The university's external media relations department will be updated along with members of the IRT on the guidelines established for the communication plan. The media relations staff will be established at the only media points of contact (POC) for handling incident communication and related aspects with the media.

4. Legal Counsel

The internal legal counselors and/or designated Risk Manager, will be responsible for the following:

- Working with external legal counselors specializing in incident response and breach management
- Fully understand potential jurisdictional issues (e.g. if a server is located in a state other than that of the main operational workplace and is attacked from a third state).
- Identify and manage any jurisdictional conflicts in the incident reporting process (Note: organizations typically should not report incidents to multiple agencies as this might result in jurisdictional conflicts).

5. Public Safety

The University's Public Safety Department will be responsible for the following:

- Be well acquainted with various law enforcement representatives and fully understand how an incident is to be reported, how the reporting is to be performed, what evidence is to be collected, and how the evidence is to be collected.
- Contact law enforcement via a designated point of contact, following the outlined protocol laid down by law enforcement.

6. Law Enforcement

Barry University, may report incidents and related information to law enforcement authorities. These may include Federal investigatory agencies, such as the Federal Bureau of Investigation (FBI), U. S. Secret Service, etc., district attorney offices and state law enforcement. Appendix E: Security Incident-Related Contacts outlines further contact details of the mentioned agencies and offices.

7. Incident Documentation

The incident response efforts at Barry University requires detailed documentation before, during and after the actual incident(s). All factual data relevant to an incident shall be recorded. Recorded data shall include all steps undertaken from the point of detection of the incident(s) to the final point of resolution.

Appendix A includes all the basic forms to be used during an incident investigation. The Incident Reporting form (A.1) is a generic form that is to be completed for an incident, regardless of category. Moreover, one specific form is to be filled out (A.2, A.3, A.4, A.5, or A.6) depending on the type of incident. For example, if a virus was reported, the Malicious Code Reporting Form (A.2) is to be filled out. In case of a multiple component incident category, the IRT members should determine the most appropriate forms to fill out.

As the investigation is carried out, additional forms are to be completed. For every action or issue detected during the investigation an Action Form (A.8) is to be filled out and the Action Tracking Log is to be completed.

It is common during an incident investigation that supporting evidence is acquired. Every time new evidence is acquired, it must be inventoried in the Supporting Evidence Inventory (A.9).

Finally, if a lessons learned “post mortem” is conducted the IRC, the Post-Incident Evaluation Form should be completed, detailing how effective the incident handling process was and identifying necessary improvements to existing security controls and practices.

The following chart summarizes the relationship between the forms:

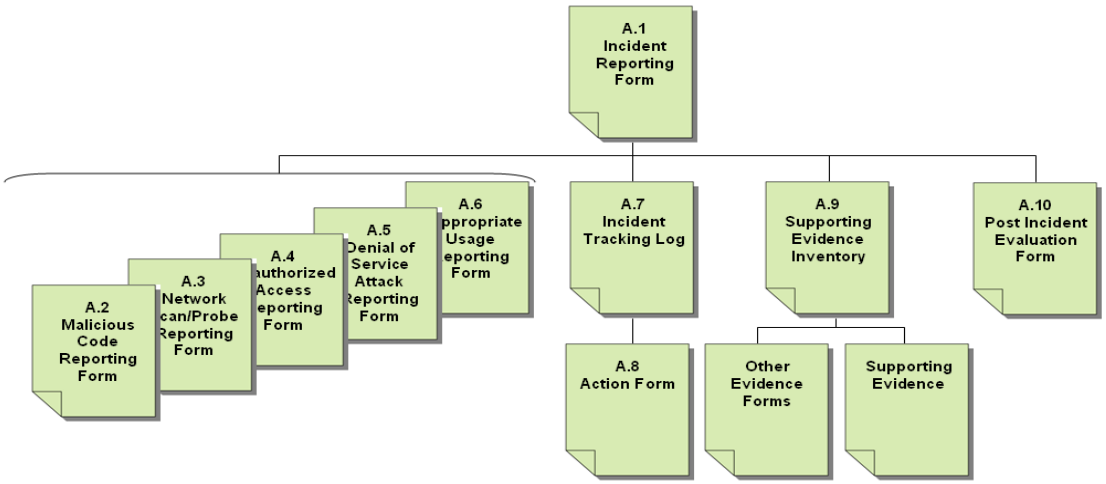

Figure 6: Relationship between Forms

8. Metrics for incident-related data

To bolster ongoing improvements in incident response capability, Barry University should consider translating all post-incident documentation into metrics to measure incident response efficiency. The following metrics should be taken into consideration:

- **Time Per Incident:** Time per incident should be measured to take into consideration the total amount of man-power resources expended on the incident, the total time from the start of the incident to its final resolution, time-lag taken for the incident response team to respond to the incident after the first alarm was raised, and the amount of time taken to coordinate with external agencies.
- **Objective Assessment:** An objective assessment should include review of logs, reports and other post-incident documentation to evaluate how well the corporate incident response policies and procedures were adhered to. This should also include an assessment of how well the incident was documented, whether the incident was detected before the damage commenced, and whether the cause of the incident was identified.
- **Subjective Assessment:** Peer reviews should be conducted after each incident as a means to evaluate incident team member performance. This should include performance before, during and after the incident(s).

Periodic audits should be conducted and should include this Computer Incident Response Program (CIRP), incident response policies and procedures, incident response team training reports, and incident response test documentation/results. The audit should also take into account the metrics defined in this section as well as incident relevant documentation and reports.

APPENDIX A: Incident Response Reporting Form

A.1 Incident Reporting Form

Incident Reporting Form	
Incident reference number:	**Report filed by:**
	Date and Time filed:
Primary Contact Information:	
Phone Number:	
Email Address:	
Incident Summary	
Date and Time of Incident Detection (specify time zone):	
Sites affected and Location:	
Incident Type: ☐ **Malicious Code** ☐ **Denial of Service** ☐ **Network Scan/Probe** ☐ **Unauthorized Access** ☐ **Inappropriate Usage** ☐ **Multiple Component** ☐ **Stolen/Lost Physical Asset**	
☐ **Other (Specify):**	
Primary affected technology and components: Host Name:_____ IP address: _____ OS Version: _____ Function of host: _____ Time Zone: _____ _____	
Other affected components including IP address and operating system version:	
Apparent source of the attack: Host Name:_____ IP address: _____ OS Version: _____ Function of host: _____	

Time Zone: _____ _____

Description of Incident (*include known facts, type of incident, damage done, sensitive information compromised or at risk, individuals in charge of incident management*):

How was the incident detected?

☐ **Automated Software** ☐ **Log Review** ☐ **System Malfunction**

☐ **3rd Party Notification** ☐ **Unknown**

☐ **Other (Specify):**

Comments (*additional details regarding the incident*):

Impact of Incident:

Remediation Action:

Incident Reported to:

Name: _____ Date/Time:_____ Signed: _____

A.2 Malicious Code Reporting Form

Malicious Code Form	
Incident reference number:	**Report filed by:**
	Date and Time filed:
Primary affected technology and components: Host Name:_____ OS Version: _____ Time Zone: _____	 IP address: _____ Function of host: _____ _____
Source of Attack: Diskette ☐ CD/DVD ☐ USB E-mail attachment ☐ Software Download ☐ Other ☐	**Type of Malicious Code:** Virus ☐ Trojan Horse ☐ Unauthorized Access ☐ Other ☐
Copy sent to:	
How was the code detected?	
Remediation actions and details	
Additional Comments:	

A.3 Network Scan/Probe Reporting Form

Network Scan/Probe Form	
Incident reference number:	**Report filed by:**
	Date and Time filed:
Date and Time of Incident Detection (specify time zone):	
Primary affected technology and components: Host Name:_____ OS Version: _____ Time Zone: _____	 IP address: _____ Function of host: _____ _____
Apparent source of the attack: Host Name:_____ OS Version: _____ Time Zone: _____	 IP address: _____ Function of host: _____ _____
Method of operation: Ports probed/scanned ☐ Order of ports or IP addressed scanned ☐ Probing tools ☐ Unique features ☐ Vulnerability Scanners ☐	**How was the incident detected?** Another site ☐ Incident response team ☐ Log files ☐ Packet sniffer ☐ Intrusion detection system ☐ Anomalous behavior ☐ User ☐ Third Party Provider ☐ Other ☐
Details:	
Supporting Evidence:	

A.4 Unauthorized Access Reporting Form

Unauthorized Access Form	
Incident reference number:	**Report filed by:**
	Date and Time filed:
Date and Time of Incident Detection (specify time zone):	
Primary affected technology and components: Host Name:_____ OS Version: _____ Time Zone: _____	IP address: _____ Function of host: _____ _____
Apparent source of the attack: Host Name:_____ OS Version: _____ Time Zone: _____	IP address: _____ Function of host: _____ _____
Method used: Sniffed/guessed/cracked password ☐ Trusted host access ☐ Vulnerability exploited ☐ Hacker tool used ☐ Utility or port targeted ☐ Social engineering ☐	**Level of access gained:**
How was the incident detected?: Another site ☐ Incident response team ☐ Log files ☐ Packet sniffer ☐ Intrusion detection system ☐ Anomalous behavior ☐ User ☐ Third Party Provider ☐	**Additional Comments**

Other ☐	
Type of information compromised (*Public, Sensitive, Confidential*)	
Supporting Evidence:	
Remediation Actions:	

A.5 Denial of Service Attack Reporting Form

Denial of Service Attack Form	
Incident reference number:	**Report filed by:**
	Date and Time filed:
Date and Time of Incident Detection (*specify time zone*):	
Primary affected technology and components: Host Name:_____ IP address: _____ OS Version: _____ Function of host: _____ Time Zone: _____ _____	
Other affected components including IP address and operating system version:	
Apparent source of the attack: Host Name:_____ IP address: _____ OS Version: _____ Function of host: _____ Time Zone: _____ _____	
Protocols involved (Other affected components including IP address and Operating System Version):	
Method of Operation: Tool used ☐ Packet flood ☐ Malicious packet ☐ IP spoofing ☐ Ports attacked ☐ Other ☐	**Details:**
Supporting Evidence:	
Remediation Actions:	

A.6 Inappropriate Usage Reporting Form

Inappropriate Usage Form	
Incident reference number:	**Report filed by:**
	Date and Time filed:
Date and Time of Incident Detection (specify time zone):	
Primary affected technology and components: Host Name:_____ IP address: _____ OS Version: _____ Function of host: _____ Time Zone: _____ _____	
How was detected?	
Type of Violation Committed:	
Description of Incident (*include known facts, type of incident, damage done, sensitive information compromised or at risk, individuals in charge of incident management*):	
Supporting Evidence:	
Remediation Actions:	

A.7 Stolen/Lost Physical Asset Reporting Form

Stolen/Lost Physical Asset Form	
Incident reference number:	**Report filed by:**
	Date and Time filed:
Date and Time of Incident Detection (specify time zone):	
Primary affected technology and components: Employee Name:_____ Type of Asset: _____ OS Version: _____ Time Zone: _____ _____	
How was detected?	
Encryption?	
Type of Violation Committed:	
Description of Incident (*include known facts, type of incident, damage done, sensitive information compromised or at risk, individuals in charge of incident management*):	
Supporting Evidence:	
Remediation Actions:	

A.8 Hardcopy Data Loss Reporting Form

Hardcopy Data Loss Form	
Incident reference number:	**Report filed by:**
	Date and Time filed:
Date and Time of Incident Detection (specify time zone):	
Primary affected documents: Employee Name:_____ Document Type: _____ Time Zone: _____	Location of Documents: _____ _____ _____
How was detected?	
Type of Violation Committed:	
Description of Incident (*include known facts, type of incident, damage done, sensitive information compromised or at risk, individuals in charge of incident management*):	
Supporting Evidence:	
Remediation Actions:	

A.9 Incident Tracking Log

Incident Tracking Log							Page of
Incident Reference Number:				**Incident/Investigation Date:** **Team Leader:**			
Action Number	**Summary of Issue**	**Proposed Issue Resolution**	**Assigned to**	**Date Assigned**	**Date to Complete**	**Date Completed**	**Action Taken**

A.10 Action Form

Action Form		
Incident Reference Number:		**Incident/Investigation Date:**
		Team Leader:
Action Title:		
Action Reference Number:	**Assigned to:**	**Date Assigned:**
Summary of the Action:		
Action Details:		
Proposed Action Resolution:		
Action Taken		
Date to Complete:		**Date Completed:**

A.11 Supporting Evidence Inventory

Supporting Evidence Inventory

Page of

Incident Reference Number:	Incident/Investigation Date: Team Leader:

Evidence Number	Date Acquired	Item Description	Acquired by	Custodian	Date Disposed	Disposition Method	Comments

A.12 Post Incident Evaluation Form

Post-Incident Evaluation Form	
Incident reference number:	**Evaluation filed by:**
	Date:
Team Members:	
Rate the incident response process on a scale of 1 – 10 (*10 being the best possible response*)	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐
How well did the Incident Response Team function as a group?	
Were procedures followed as per documentation? Any suggestions for improvement?	
Any changes suggested in work steps to better respond to the incident in the future?	
Any additional resources that could make the incident response process more efficient?	
Other suggestion, recommendations or comments:	

APPENDIX B: Security Incident Contact List

IRT Role	Name	Phone Number	Mobile Number	Pager Number	Email Address	Office Address

APPENDIX C: Checklist

Preparatory Steps

- ✓ Ensure that the forms included in the Appendix A are available to each team involved in the incident response process.
- ✓ Ensure that the Security Incident Contact List in Appendix B is updated and available to each team involved in the incident response process.
- ✓ Ensure that the escalation procedure outlined in this document is provided to every team involved in the incident response process.
- ✓ Ensure that the security incident response procedures are available to each team involved in the incident response process.
- ✓ Create free e-mail accounts with well-known providers (i.e. Hotmail, Yahoo, etc.) per team involved in the incident response process. These accounts are to be used in the event that the corporate e-mail becomes unavailable. The content of messages transmitted through this communication channel should be strictly limited to tactical operations related to the containment of an incident.
- ✓ Provide a physical copy of Appendix E - Security Incident-Related Contacts to each team involved in the incident response process.
- ✓ Provide ongoing training to operational and support staff relevant to handling security incidents.
- ✓ Implement and effectuate incident response training drills on an ongoing basis to ensure that employees and incident response teams are familiar with the incident response process and the associated policies and procedures.

Response Steps

- ✓ Attempt to contain the incident and keep a note of its timing, duration and location. Also attempt to find out if the incident is ongoing and if there is a need to isolate affected systems/devices.
- ✓ If the incident shows signs of resulting in a legal investigation at a later stage, follow all necessary forensic practices to ensure that any evidence collected will be permissible in a court of law.
- ✓ Attempt to determine the extent of damage caused by the incident. Get in touch with relevant third parties (e.g. Internet Service Provider, etc.) to see what evidence can be obtained from their end.
- ✓ During recovery, perform technical upgrades/patches deemed necessary, perform a thorough vulnerability assessment and configuration review, harden

the network both from an external and internal perspective, and perform a thorough review of the policies and procedures.

- ✓ Start managing public relations and publicity issues with internal employees, customers, and shareholders, and also manage the necessary interactions with the police, investigative agencies, regulatory bodies and insurers.
- ✓ Ensure that you hold an internal meeting to inform employees about the incident.

APPENDIX D: Tools and resources available

Incident Response-Related Mailing Lists

List	URL	Responsibility Assigned
Bugtraq	http://www.securityfocus.com/archive/1	
Current Activity	http://www.us-cert.gov/current/	
Cyber Security Alerts	http://www.us-cert.gov/cas/alerts/	
Cyber Security Bulletins	http://www.us-cert.gov/cas/bulletins/	
Cyber Security Tips	http://www.us-cert.gov/cas/tips/	
DShield	http://www.dshield.org/pipermail/list	
Focus on IDS	http://www.securityfocus.com/archive/96	
Forensics	http://www.securityfocus.com/archive/104	
Incidents	http://www.securityfocus.com/archive/75	
Intrusions	http://cert.uni-stuttgart.de/archive/intrusions	
Log Analysis	http://airsnarf.shmoo.com/pipermail/loganalysis	
National Cyber Alert System	http://www.us-cert.gov/cas/	
Technical Cyber Security Alerts	http://www.us-cert.gov/cas/techalerts/	

Technical Resources

Resource	URL	Responsibility Assigned
Center for Education and Research in Information Assurance and Security (CERIAS) Intrusion Detection Pages	http://www.cerias.purdue.edu/about/history/coast/archive/data/category_index.php	
Clearing House for Incident Handling Tools (CHIHT)	http://chiht.dfn-cert.de	
CSIRT Development, CERT®/CC	http://www.cert.org/csirts	
Computer Security Resource Center (CSRC), NIST	http://csrc.nist.gov	
Distributed Intrusion Detection System (DShield)	http://www.dshield.org	
Incident Handling Links and Documents	http://www.honeypots.net/incidents/links	
Intrusion Detection FAQ, SANS Institute	http://www.sans.org/resources/idfaq	
Intrusion Detection Links and Documents	http://www.honeypots.net/ids/links	
Loganalysis.org	http://www.loganalysis.org	

Vulnerability Resources

Resource	URL	Responsibility Assigned
CERT®/CC Advisories	http://www.cert.org/advisories	
CERT®/CC Incident Notes	http://www.cert.org/incident_notes	
CERT®/CC Vulnerability Notes	http://www.kb.cert.org/vuls	
CIAC Bulletins and Advisories	http://www.ciac.org/cgi-bin/index/bulletins	
Common Vulnerabilities and Exposures (CVE)	http://www.cve.mitre.org	
National Vulnerability Database (NVD)	http://nvd.nist.gov/	
Open Vulnerability Assessment Language (OVAL)	http://oval.mitre.org/	
Packet Storm	http://www.packetstormsecurity.com	
SANS/FBI Top 20 List	http://www.sans.org/top20	
SecurityFocus Vulnerabilities Database	http://www.securityfocus.com/bid	

Other Resources

Resource	URL	Responsibility Assigned
8LGM	http://www.8lgm.org/advisories.html	
Automated Systems Security Incident Support Team (ASSIST)	ftp://ciac.llnl.gov.pub/ciac/secdocs/assist	
ISS Xforce	http://xforce.iss.net/	
Microsoft Security Advisory	http://www.microsoft.com/security/default.asp	
Sun Microsystems Advisory	gopher://fas-gopher.harvard.edu/11/.abcd/.security/.sun	

APPENDIX E: Security Incident-Related Contacts

Reporting Computer Hacking, Fraud and Other Internet-Related Crime

Crime	Appropriate Agencies
Computer Intrusion (Hacking)	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm) • U. S. Secret Service (http://www.treas.gov/usss/index.shtml) • Internet Crime Complaint Center (http://www.ic3.gov/)
Password trafficking	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm) • U. S. Secret Service (http://www.treas.gov/usss/index.shtml) • Internet Crime Complaint Center (http://www.ic3.gov/)
Counterfeiting of currency	• U. S. Secret Service (http://www.treas.gov/usss/index.shtml)
Child Pornography or Exploitation	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm) • If imported, U. S. Immigration and Customs Enforcement (http://www.ice.gov/) • Internet Crime Complaint Center (http://www.ic3.gov/)
Child Exploitation and Internet Fraud matters that have a mail nexus	• U. S. Postal Inspection Service (http://www.usps.com/postalinspectors/) • Internet Crime Complaint Center (http://www.ic3.gov/)
Internet fraud and SPAM	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm) • U. S. Secret Service (Financial Crimes Division) (http://www.treas.gov/usss/financial_crimes.shtml) • Federal Trade Commission (Online complaint) (http://www.ftc.gov/) • If securities fraud or investment-related SPAM e-mails, Securities and Exchange Commission (http://www.sec.gov/complaint.shtml) • Internet Crime Complaint Center

Crime	Appropriate Agencies
	(http://www.ic3.gov/)
Internet harassment	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm)
Internet bomb threats	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm) • ATF Local Office (http://www.atf.gov/field/index.htm)
Trafficking in explosive or incendiary devices or firearms over the Internet	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm) • ATF Local Office (http://www.atf.gov/field/index.htm)

Reporting Intellectual Property Crime

Crime	Appropriate Agencies
Copyright piracy (e.g. software, movie, sound recordings, etc.)	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm) • U. S. Immigration and Customs Enforcement (http://www.ice.gov/) • Internet Crime Complaint Center (http://www.ic3.gov/)
Trademark counterfeiting	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm) • U. S. Immigration and Customs Enforcement (http://www.ice.gov/) • Internet Crime Complaint Center (http://www.ic3.gov/)
Theft of trade secrets	• FBI Local Office (http://www.fbi.gov/contact/fo/fo.htm)

Incident Response Organizations

Organization	Website
Computer Crime and Intellectual Property Section (CCIPS), U. S. Department of Justice	http://www.cybercrime.gov
CERT® Coordination Center (CERT®/CC), Carnegie Mellon University	http://www.cert.org
CERT®/CC Incident Reporting System	http://irf.cc.cert.org
Computer Incident Advisory Capability, U. S. Department of Energy	http://www.ciac.org/ciac
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org
Government Forum of Incident Response and Security Teams (GFIRST)	http://www.us-cert.gov/federal/gfirst.html
High Technology Crime Investigation Association (HTCIA)	http://www.htcia.org
IETF Extended Incident Handling (inch) Working Group	http://www.ietf.org/html.charters/inch-charter.html
Internet Storm Center (ISC)	http://isc.incidents.org

United States Computer Emergency Response Team (US-CERT)	http://www.us-cert.gov
US-CERT Incident Reporting System	https://forms.us-cert.gov/report

APPENDIX F: Breach Notification

The following is a selected statue relating to the breach of personal information about an individual. This section should not be considered a complete list. *Note: all 47 state breach notification laws must be reviewed (as applicable) for each unique incident*.

I. Florida Information Protection Act of 2014 - **Florida Statutes Annotated § 501.171 (effective July 1, 2014)** (excerpts)

"**Breach of security**" or "**breach**" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

"**Personal information**" means either of the following:
a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:
(I) A social security number;
(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Notice to Individuals of Security Breach
A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that

was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized by law enforcement.

The notice to an affected individual shall be by one of the following methods:
1. Written notice sent to the mailing address of the individual in the records of the covered entity; or
2. E-mail notice sent to the e-mail address of the individual in the records of the covered entity.

Notice to the Department of Legal Affairs (Attorney General). Notice must also be provided to the Department of Legal Affairs (Florida Attorney General if there are more than 500 impacted individuals.

II. HITECH Breach Notification

Final breach notification regulations, effective for breaches discovered on or after September 23, 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act and finalized by the Omnibus Bill, effective March 23, 2013, by requiring HIPAA covered components and their business associates to provide notification following a breach of ***unsecured*** protected health information.

Under the Omnibus (Final) Rule, a breach is *presumed* if there is an impermissible acquisition, access, use or disclosure of PHI unless the Company (as either Covered Entity or Business Associate) demonstrates a low probability that PHI has been compromised, based on the following four (4) risk factors:

(1) The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;

(2) The unauthorized person who used the PHI or to whom disclosure was made;

(3) Whether PHI was actually acquired or viewed; and

(4) The extent to which the risk to PHI has been mitigated (i.e., obtaining reliable assurances by a recipient of PHI that the information will be destroyed or will not be used or disclosed).

The regulations, developed by the Office for Civil Rights, require HIPAA covered components to promptly notify affected individuals of a breach of their protected health information, as well as the Health and Human Services (HHS) Secretary and the media in cases where a breach affects more than 500 individuals.

Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis (by March 1st of the following calendar year of the breach). The regulations also require business associates of covered components to notify the covered component of breaches at or by the business associate or its workforce, agents or subcontractors.

APPENDIX G: Definitions

- **Access** – logical/physical communication or contact with a technical infrastructural element.

- **Denial of Service** – Refers to Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks. This is an attacks technique wherein computing resources are consumed for non-intended purposes, thus preventing normal/legitimate use of the computing resources for their originally intended functions.

- **Event** – An observable occurrence in a technical infrastructure.

- **Forensic** – Refers to activities related to *Computer Forensics*. Involves gathering, retaining and analyzing digital data for investigative purposes, at the same time maintaining the integrity of the data.

- **Incident** – Refers to a *computer security incident*. This is a violation or an imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

- **Incident Response** – Mitigation of an *incident* with an attempt to reduce risks to an acceptable level.

- **Network Probe** – Also referred to as a *Port Scan*. This involves automated or manual methods to determine which ports on a system(s) are open, thus enabling an attacker to obtain information for subsequent attacks.

- "**Personal information**" means either of the following:

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

- **Protected Health Information** - confidential information that is created, received, and/or maintained related to an individual's health care (or payment related to health care) that directly or indirectly identifies the individual

- **Risk** – The probability of an *incident* occurring.

- **Threat** – The potential source of an *incident*.

- **Virus** – A self-replicating program that runs and spreads by modifying other programs and/or files.

- **Vulnerability** – A weakness in a technical infrastructural element that can be subject to exploitation or misuse.

- **Worm** – A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.