Grayson College
Incident Response Plan

Contents

About This Incident Response Plan

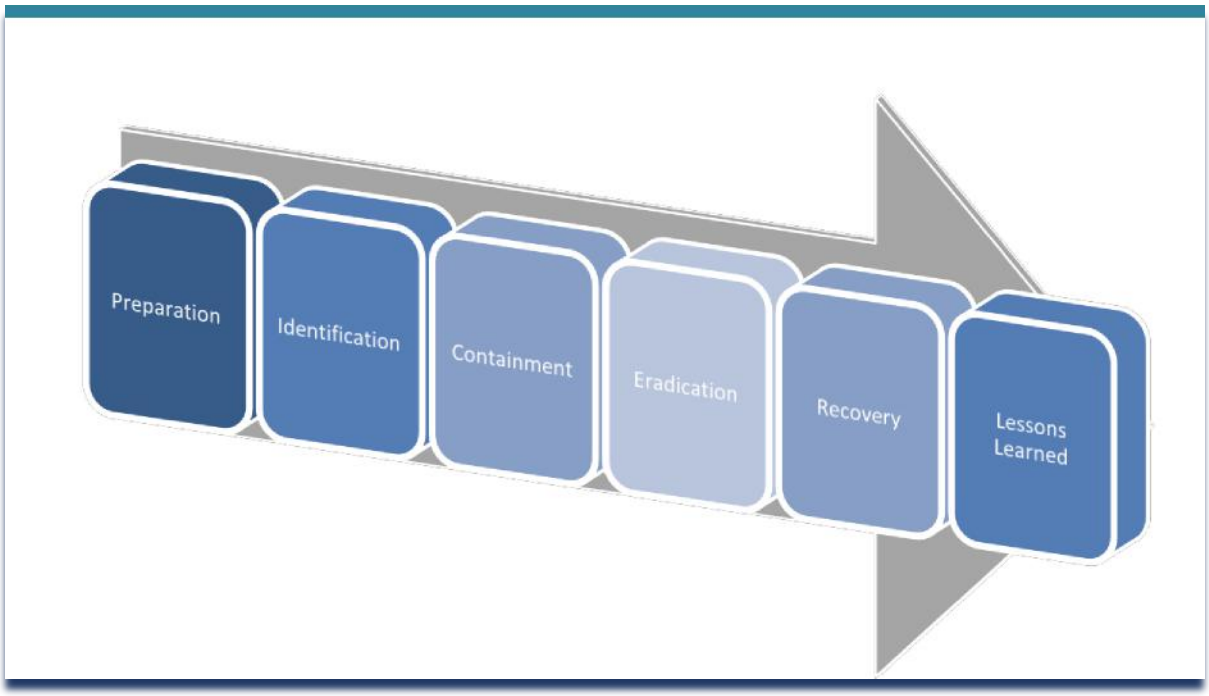
History

Version No.	Issue Date	Status	Reason for Change
v1.0	10/15/2020	Draft	

Review

Reviewer's Details	Version No.	Date

1 Introduction to the Incident Response Plan



The Incident Response Plan (“IRP”) is intended to provide an organized, well-defined approach for responding to critical Security Incidents affecting Grayson College’s electronic information assets. This Incident Response Plan shall be implemented by the College’s Incident Response Team, which consists of a group of designated Grayson College employees tasked with the responsibility of responding to critical Security Incidents, including ensuring remediation of the Security Incident and recommending controls to prevent further Security Incidents from reoccurrence. The Grayson College Incident Response Team shall utilize this plan to assess the significance of an incident based on the operations impact on the affected resources and the current and potential technical effect of the incident (e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks).

1.1 Scope

All authorized users have an interest in the security of college resources at Grayson College, and share in the responsibility for protection of those resources, prevention of problems, and incident detection and response. This IRP covers the response to critical Security Incidents that threaten the confidentiality, integrity, and availability of Grayson Colleges electronic information assets, as well as Grayson Colleges systems, networks, and media that collect, process, store, and deliver such information. It applies to critical Information Security incidents of all types and is applicable to employees, contractors, vendors, and other persons and/or organizations that perform technology functions in support of the College, including systems, network, desktop, and applications. Grayson College’s Written Information Security Program, Information Handling, Backup and Retention Standard, and Business Continuity & Disaster Recovery Policy apply to this process.

1.2 Compliance

Failure to comply with the requirements in this process is grounds for disciplinary action, up to and including termination of employment, cancellation of consultancy or contractor arrangement, termination of business contract, civil action and/or criminal prosecution. In cases where there is a conflict between this process and other Information Security Policies and Procedures, the more stringent requirement applies. Every attempt should be made to follow the Incident Response process.

1.3 Audience

This document is intended for technology personnel involved in responding to security events.

1.4 Responsibilities

Executive Sponsor

- College President
- Vice President for Information Technology (VP-IT)

Key Stakeholders

- Local Support Providers
- Grayson College Business Services
- Grayson College Communication Director
- Grayson College Network Services
- Information Technology Security Managers
- 24/7 IT Support Center
- Vice President of Student Affairs
- College Director of Campus Safety
- Vice President of Instruction
- College Marketing and Public Information
- Legal Counsel

IRP Owners & Assumptions

The Information Security Incident Response Plan Lead and the Vice President of Information Technology (VP-IT) are responsible for publishing this Incident Response Plan (IRP) in order to provide the Incident Response Team (IRT) with guidance on how to respond to security incidents. This guidance is provided with the following assumptions:

- The details of a security incident cannot be predicted with any accuracy
- No two security incidents are identical
- The social and/or political climate in the world is dynamic and may, at times, impact operations requirements
- Information Security Incident Response effectiveness is dependent upon consistent management of the response activities

Due to the aforementioned assumptions, these guidelines are provided as a framework in which to respond to critical security incidents. For the IRT to be effective it must dynamically respond to individual situations in an appropriate manner as experience and expertise allow. Further guidance regarding appropriate actions to take in situations not adequately addressed in this document, will be provided by the IRT when required.

This IRP is intended to be a living document, and will be regularly tested and reviewed annually. The IRP will be updated as appropriate, under the supervision of the Incident Response Plan owner and the direction of the VP of IT. Additionally, this plan shall be modified accordingly, in response to lessons learned from incidents and to incorporate industry developments. This document is also governed by all applicable Grayson College policies and procedures.

Employee Security Incident Reporting Policy

The Incident Response Plan Owner and the College's Vice President for Information Technology (VP-IT) are also responsible for ensuring that Grayson College publishes and maintains the process for Incident Reporting. This process must provide Grayson College's workforce with appropriate guidance and an effective and secure communications channel to report security incidents. Additionally, the Incident Response Plan owner and the VP-IT must ensure that, as technology advances and Grayson College's supporting security documentations change, the employee reporting instructions and mechanisms remain appropriate. The Grayson College's supporting security documents are listed In **Appendix A.**

1.5 Definitions

Acronym/Phrase	Definition
IRT	Incident Response Team, See Section 2. See also **Appendix B** for the list of members of this team. To obtain Team Member telephone numbers and email addresses reference the Corporate Intranet. See “Incident Response Team”
Computer Emergency Response Team	The team of Carnegie-Mellon researchers involved with analyzing and recommending courses of action with worldwide computer incidents.
Virtual Security Incident Response Team	The team is comprised of key Grayson College personnel who have subject matter expertise for identifying threats to their area, such as Windows, UNIX, routers, LAN/WAN, Extranet, NT/2000/UNIX, Databases (Oracle and SQL server), etc**.**
Critical Security Incident	A Security Incident with a severity classification defined as High Risk / Level One.
Incident	See “Security Incident”
Incident Details	Incident Details to be prepared for each Security Incident as outlined in **Appendix C.**
Information Asset	Any data or information collected, obtained, processed, used, communicated, and/or stored by Grayson College in electronic form. Information Assets include, but are not limited to, Personally Identifiable Information.
IR Team Leader	Individual responsible for coordinating team members and activities during an incident
IRP Plan	Information Security Incident Response Plan
Personal information	See “PII”
PII	Personally Identifiable Information- Information about an identified or identifiable individual, including but not limited to: name, address, e-mail address, date of birth, telephone number, Social Security number, employee identification number, driver’s license or other government issued identification number, customer number, financial account number (including bank account or credit/debit card number), mother’s maiden name, medical information, financial information, and other similar information.
Plan	See “IRP”
POC	Point of Contact

Security Incident	Any irregular, adverse, or uncontrolled event that threatens the confidentiality, integrity, or availability of any Grayson College information asset, system, network or storage media, or any violation or imminent threat of violation of any Grayson College computer security policies, acceptable use policies, or standard security practices. Examples include but are not limited to: • Denial of service attacks that prevent or impair the authorized use of Grayson College information assets, systems or networks, such as by exhausting resources with the specific intent of interrupting or interfering with their operation • Malicious code, such as a virus, worm, Trojan horse, or other malware that infects a Grayson College system • Unauthorized access or modification to any Grayson College information asset, system, network or storage media, such as where an internal or external person gains (or attempts to gain) access without permission to Grayson College data, systems, networks, or storage media, including by using someone else's password, social engineering, misuse of authority, stealing, copying, or otherwise misusing or misappropriating data, hacking, network probes, or port scanning attempts • Inappropriate use or modification of Grayson College information assets, systems, or networks, or storage media such as employee misuse or disclosure of information, employee theft or other misconduct whereby a person violates acceptable use policies • Loss or theft of equipment (e.g., laptops) or media (e.g., USB drives) containing Grayson College information assets • Critical alerts from intrusion detection systems, intrusion prevention systems, and file integrity monitoring systems • Any other compromise or violation of, or imminent threat to, any Grayson College information asset, system, network, or storage media, or violation of any Grayson College computer security policy, acceptable use policy, or standard security practices.
Security Incident Severity Classifications	Incidents are classified by severity into three (3) classes (High Risk- Level One, Medium Risk- Level Two, Low Risk- Level Three) in order to determine the appropriate response and to identify the impact on Grayson College's operations. See descriptions of each Security Incident Severity Classification in **Appendix E**.

1.6 Trademarks

The following trademarks are referenced within this document:

- Computer Emergency Response Team (CERT) – Copyright by Carnegie-Mellon

1.7 Documents and Maintenance

The Incident Response Team and the Information Technology Office maintain this document. It is a controlled document. Any changes to this document must undergo a formal review process with representation from both teams.

Because Incident Response is a mature process, it will be reviewed annually by division leaders or as dictated by operational need.

The IRP Owner will initiate a review of the process based on the following factors:

- Request from the vice President for Information Technology to review the process
- Modification to standard IR methodologies
- Twelve months have elapsed from the previous review of the Computer Incident Response process
- Results of compliance audits require modifications to the process to remediate noted exceptions and control deficiencies

2 Incident Response Team (IRT)

2.1 Overview

The IRP owner is required to ensure that the capability exists to respond to incidents at all Grayson College locations. This capability will be provided by a formal Incident Response Team (IRT). This team will be comprised of technical resources with the appropriate skills to identify, assess, respond to and communicate the effects of security incidents. IRT members will be designated by the VP-IT with approval by the College President, who is authorized under the Information Security Policy to act in the best interest of the College to secure resources that are actively threatened and to abide by the incident handling procedures to mitigate the threat. Full cooperation with the IRT is required of all authorized users of college resources. The team will incorporate or coordinate when appropriate with representatives from the following departments:

- Legal (Privacy)
- Information Technology
- Information Security
- Human Resources

The IRT is a reactive, investigative body only and is convened strictly for handling and investigating serious system interruptions and/or a potential or actual security incident. The role of the IRT is to respond rapidly by:

- Identifying the type of situation
- Identifying, if possible, the cause
- Containing the damage/exposure
- Preserving the evidence properly
- Successful remediation or eradication of the threat
- Identifying the individuals involved, as applicable
- Presenting post-resolution issues and recommended solutions to management
- Assisting OGC and law enforcement in matters of litigation/prosecution, as applicable
- Notifying/training users of proper procedures to control a Security Incident

By being prepared to respond to critical incidents, the IRT can minimize damage to college computer systems, networks and data.

The members of the IRT are listed in **Appendix B**. The IRT will be assembled as needed and will operationally report to the IRP owner.

All response activities for Level One security events must be handled by the IRT and managed by the IRP owner at the direction of the Vice President for Information Technology. The IRP owner will function as the central clearing house and management office of all IRT incident response activities and internal and external communication regarding such incidents.

2.2 IRT Response Capabilities

The IRT must be prepared to deal with all threats facing Grayson College's information assets and information technology infrastructure. The following paragraphs outline the primary capabilities required.

Technical Capabilities

The IRT must have the technical expertise to respond to critical security incidents involving any and all components of the information technology infrastructure. If appropriate internal personnel are not available to assist the IRT, the VP of IT must have arrangements in place for external personnel to augment the IRT as required.

Internal Coordination

To facilitate effective and secure internal communications, the IRP owner must maintain an up-to-date roster of internal personnel assigned to the IRT for both support, and ad hoc team members. Additionally, the IRP owner must develop and maintain a communications plan to assemble the IRT promptly when needed, and to facilitate secure communications between IRT members and coordinators throughout the response process.

2.3 IRT Roster & Responsibilities

There are three types of members who will comprise the IRT team, core members, support members, and ad hoc members. The Vice President of Information Technology will identify the core members and appoint the team leader.

The Core team members will convene when a security incident is suspected. They will be responsible for:

- Determining the level of severity of the security incident
- Determining if the security incident warrants further investigation
- Categorizing the security incident
- Adding support members to the investigation, if necessary

The Support team members will not be full-time members of the IRT. These members have valuable expertise in their fields. When the core team determines that the investigation requires the added expertise of a support member, that member will be added to the team for the duration of the investigation.

Similar to the Support team members, the Ad-hoc team members will not be full-time members of the IRT. These members will be engaged when an incident requires the specific discipline owned by the ad-hoc team member.

Core Team Members

IRP Owner (IRT Project Lead) is responsible for:

- Providing operational direction and oversight to the IRT under the direction of the Vice President of Information Technology
- Central Point of Contact (POC) for the IRT

- Receiving initial incident reports provided by security personnel
- Responding to all reported critical security incidents both internally and externally
- Reporting status and progress to the Leadership Team
- Tracking, reviewing and ensuring that appropriate action is taken in response to security incidents
- Interacting with all members of IRT, including director and executive level members to provide recommendation and assistance as needed related to all areas under the scope of IRT
- Reviewing new vulnerabilities and exploits, including new viruses released 'in the wild' and alert relative teams as necessary
- Documenting and managing all special projects and process flows that improve Grayson College infrastructure covered under the scope of IRT (e.g., Virus Reporting, MS Updating)

IRT SME is responsible for:

- Assisting the Project Lead in the creation of new processes and standards, reporting, special projects and functions as triage points in data gathering for their CMCs
- Providing technical documentation as needed
- Providing advanced level of support to 24/7 IT Support Center when needed for issues that fall within the scope of IRT
- Monitoring infections to ensure compliance with all security applications
- Offering disaster assistance and research on all Virus/Vulnerability (Level 1) events

Vice President for Information Technology is responsible for:

- Assembling, coordinating and maintaining the IRP & IRT with the assistance of the IRP owner
- Ensuring appropriate education and training is provided for all IRT personnel
- Providing approval for all documents developed by the IRP owner
- Ensuring appropriate communication plan is in place based on the specific incident's scope

Support Team Members

IT Staff Manager is responsible for:

- Collaborating with IT Leaders and IT employees at the direction of the IRP owner to ensure that appropriate action is taken in response to security incidents
- Managing relevant technology to assist in alerting on potential incident events
- Managing relevant technology to assist in event reconstruction
- Providing forensic assistance when necessary

Local Support Provider is responsible for:

- Collaborating with IT Leaders and IT employees at the direction of the IRP owner to ensure that appropriate action is taken in response to security incidents
- Managing relevant technology to assist in alerting on potential incident events
- Managing relevant technology to assist in event reconstruction
- Providing forensic assistance when necessary
- Implementation of all IRT approved Security Updates to workstations in the, as per the CMR process
- Testing, approving and applying all IRT approved Security patches to all workstations
- Ensuring virus software compliance based on standardized documentation
- Reporting all incidents, problems or questions to the IT Staff Manager or SME, including issues that would cause non-compliance with all IRT standards or incur possible outages based on virus or exploit activity

Monitoring Teams are responsible for:

The teams within this category monitor infrastructure views into Grayson College network including Patching and AV Health. These groups include:

- Server Operations
- System Engineering
- Security Operations
- 24/7 IT Support Center

Ad-hoc Team Members

Director of Human Resources is responsible for:

- As requested by the IRP owner, coordinating and assisting the IRT in the response of security incidents
- Consistent application of disciplinary actions in accordance with this and other corporate policies
- Facilitating internal communications where applicable

College Communications member is responsible for:

- As requested by the IRP owner, coordinating and assisting the IRT in the response of security incidents
- Providing appropriate internal and external communications regarding security incidents, following consultation with relevant internal stakeholders and approval from the IRP owner and the Information Security Officer

Legal Counsel member is responsible for:

- As requested by the IRP owner, coordinate and assist the IRT in the response of security incidents as it relates to Legal intervention
- Providing Attorney-client privilege communication in an effort to assist the investigation from the perspective of a lawful manner
- Obliging the investigation with local and/or state law enforcement agencies as necessary

Risk/Compliance member is responsible for:

- As requested by the IRP owner, coordinate and assist the IRT in the response of security incidents as it relates to Risk and Compliance amongst the organization
- Determine the Risk Level impact to the wide organization as necessary

Business Continuity / Disaster Recovery member is responsible for:

- As requested by the IRP owner, coordinate and assist the IRT in the response of security incidents as it relates to impacted College operations
- Determining the means to restore and recover the impacted application or system

3rd Party Vendor member is responsible for:

- As requested by the IRP owner, coordinate and assist the IRT in the response of security incidents as it relates to the application or system impacted

Grayson College Employees

Grayson College Leaders and Grayson College employees, while not part of the IRT, are responsible, as requested by the IRP owner and the Information Security Officer for coordinating and assisting the IRT in the response of security incidents

3 Initial Reporting, Classification, and Response

3.1 Initial Reporting of a Security Incident

All employees must promptly report all actual, potential and suspected High Severity (**Level 1**) Security Incidents to the IRP owner. Authorized users should be instructed to contact the Help Desk or an IT Leader as soon as they become aware of, or suspect, a potential or actual Security Incident.

When a Security Incident is reported, an IT Leader, under the supervision of the IRP owner must promptly:

- Gather Incident Details as specified in **Appendix C**.
- Conduct an initial *evaluation* of the Security Incident to assess its Severity Classification; and
- If appropriate, escalate the Security Incident to the IRP owner or IRT SME and assist in conducting an initial analysis and investigation of the Security Incident and determining the appropriate Security Incident Severity Classification.

Archive of Incident Records

All Security Incident Records must be continually updated throughout the life of the Security Incident as information becomes available, and thereafter must be archived by the IRP owner to facilitate long and short-term trend analysis of:

- Internal and external vulnerabilities
- Target hosts
- Originating hosts, domains and networks
- Techniques used in the course of attacks
- Procedural or administrative problems that facilitated the Security Incident

The Security Incident Archive is a source of information that details security incidents. At a minimum, the Security Incident Details in this archive must contain the (known) information set forth in **Appendix C**.

The employees performing the initial analysis function will know only a portion of this information; the remainder of the information will be entered into the database during the course of the investigation and response.

3.2 Initial Analysis and Triage

Upon notification of a potential security incident, an IT Leader must promptly review all available information related to the Incident and make an initial evaluation of its Severity Classification. It is expected that this triage function will begin by contacting the user or users who reported the issue. This initial review is conducted to quickly evaluate the severity of the situation, assist in the assignment of the Severity Classification, and recommend the next step in response to the Security Incident, including immediate or emergency response actions if warranted.

An example of an emergency response action is shutting down mission critical systems, services, or network components to halt the spread of viruses, worms, or significant threats to College or an external organization's information technology infrastructure. Extreme measures such as shutting down key components of Grayson College information technology infrastructure should only be taken with approval of the IRP owner, and Information Security Officer.

Unless it is clear that the Security Incident is a Low (Level 3) or Medium Risk (Level 2) Incident, the IT Leader must promptly escalate it to the IRP owner and, if necessary, along with the Information Security Officer, further review, evaluate, and designate a Severity Classification for the incident for the determination of next steps.

3.3 Classification of a Security Incident

Promptly after a Security Incident is reported, the Security Incident Response Core Team should determine the appropriate Severity Classification as Level one, two, or three, according to the severity of the situation as outlined in **Appendix D**. In determining whether the impact of a Security Incident will be significant, moderate, or minor, as required for the classification process, consideration should be given to:

- The nature and extent of the Security Incident
- Importance of the information and/or system affected
- The overall effect of the Security Incident on Grayson College information technology infrastructure
- Resources required to remedy the situation
- Overall effect of the Security Incident on the business processes supported
- Potential or realized disclosure of Grayson College proprietary information or personally identifiable information
- The type and sensitivity of the information involved
- The potential harm to Grayson College, and to any other affected individuals, that has, or may result
- The legal impact of the Security Incident

The Information Security Officer may delegate to the IT Leaders the authority to make determinations that Security Incidents are Low Risk (Level 3) in those cases where the facts clearly support such a classification.

3.4 Activation of the Security Incident Response Team

The response activities must be prioritized in accordance with the Severity Classification assigned to a Security Incident. The IRT must be activated under either of the following conditions:

- A Security Incident has been classified as a **Level 1,** or
- At the request of the Information Security Officer

In either case, the IRP owner will initiate the Security Incident Response processes, the IRT must be notified, and the IRT will be responsible for responding to the Security Incident.

Once the IRT has been activated, it will promptly convene in person, or via teleconference, to assess the conditions of the Security Incident, begin recording all of the relevant facts, and begin the response process.

If the Security Incident has been classified as a **Level 3 or Level 2**, the handling of the Security Incident should be directed to the appropriate department. For example, if the Security Incident involves one computer with an easily controlled virus, the Local Support Provider should handle the response. However, the Local Support Provider should nonetheless document the Security Incident and the response and submit a final Incident Details summary regarding the Security Incident immediately after the Security Incident is resolved, to the Security Incident Response Plan owner.

Note that as the investigation of a Low or Medium Risk Security Incident progresses, the Security Incident should be reclassified if additional facts are discovered indicating that the Security Incident Severity Classification should be raised which could trigger the need to contact the IRT.

3.5 IRT Response Assignment

In situations where the IRT has been activated, the IRP Plan owner must designate a IRT member as the lead response handler. The lead handler will direct the response and serve as the primary communication channel internally for the particular situation. The designation of the lead handler will be made by the IRP Plan owner based on the following criteria:

- Technical Expertise – Not all IRT members will be proficient with all components of College information technology infrastructure, therefore assignment of lead must favor the employees with the most qualifications and experience to handle a particular situation.
- Workload – As the frequency of security incidents cannot be reliably predicted, assignment of lead for any particular situation must account for any concurrent response activities as well as other work duties performed by IRT members.
- Response Experience – As there will be varying degrees of response experience among the IRT members, preference should be given to more experienced employees for situations of higher severity or complexity.
- A duty roster of IRT members should be maintained to provide for the response to situations on an after-hours basis. This roster should define terms of responsibility for after-hours response. The identified duty employees should ensure that the triage functionary is able to promptly contact him/her at all times throughout the duty term.

4 Response Procedures

The following is a general guideline outlining appropriate response procedures for the IRT.

4.1 Initial Response

Once the IRT has been assembled and made aware of the suspected critical Security Incident, it must assess the circumstances and details surrounding the Security Incident. This includes verifying that a critical Security Incident has actually occurred, and identifying (i) what information assets are affected, (ii) which systems, networks, and/or locations are affected, (iii) which users are involved, and (iv) the potential operational impact. The IRT should verify enough information about the Security Incident so that an overall response strategy can be formulated.

The IRT must also determine the most appropriate response strategy, given the circumstances of the Security Incident. The strategy should take into consideration technical, operations, and legal factors. Because the response strategy can have repercussions that influence employees, partners and customer confidence, it should be approved by IRP Plan owner and the Information Security Officer.

Factors that should be considered in deciding how to respond to the Security Incident include the following:

- When the Security Incident occurred and when it was discovered
- How critical the affected systems are
- The sensitivity of any compromised or stolen information
- Who the potential perpetrators are
- Whether or not the Security Incident is known to the public or should or must be disclosed to the public or other third parties
- The level of unauthorized access attained by the perpetrator
- The apparent skill of the perpetrator
- How much system and user downtime can be tolerated
- The overall dollar loss involved
- Potential legal obligations.

Note that a much more detailed investigation (described below) may be necessary before finalizing a particular response strategy.

Response Priorities

The IRT must take the necessary steps to protect the integrity of the information related to any security incident. This information can be useful in developing countermeasures for security vulnerabilities and may be required for corporate disciplinary actions, civil litigation, and/or criminal prosecutions. Nonetheless, the IRT will always function with respect to the following priorities:

- Preserve life
- Prevent physical damage to personnel, facilities, or systems
- Prevent financial loss
- Prevent logical damage to systems and networks
- Improve security of the information technology infrastructure
- Protect evidence

4.2 Time Tracking

Throughout the course of any incident response, it is critical for the IRT to be able to quantify all time spent on the situation. Employee's time allocation is one of the primary factors in determining the cost of an incident. In many cases, where little logical and no physical damage is done to systems, it is the only factor that determines the cost of the Security Incident. The cost of responding to incidents is an important metric that must be quantified for the following reasons:

- Many Cyber Insurance providers require detailed tracking of hours during a claim
- Grayson College's Cyber Insurance Policy requires notification if an event occurs. This notification would be decided on between Grayson College President, Vice President for Information Technology. and Legal Counsel (if necessary). Claims can be started via the form found in Appendix H.
- Grayson College management must understand the costs associated with Information Technology, and Information Security for budget planning and analysis
- The IRP Plan owner and Information Security Officer, with the assistance of the IT Staff Manager, must be aware of the costs associated with incidents to evaluate potential capital expenditures and the expected ROI for products or services designed to reduce the number or severity of security incidents.
- Law Enforcement organizations generally require a cost threshold to be met prior to committing their resources to any investigation

The generally accepted rule to determine the costs associated with a security incident is as follows:

- For employees who assisted in the response: *Divide the yearly salary of the employee by 2080, and then multiply the quotient by the number of hours spent on the response*
- For contractors or consultants: *simply multiply the hourly rate by the hours spent on the response*
- *Add sums for all individuals involved to derive the total employee's costs*

4.3 Situation Assessment

The investigation phase determines the who, what, when, where, and how surrounding the Security Incident. After determining Grayson Colleges approach in responding to the Security Incident, the IRT should begin its investigation and assign resources (personnel and financial) to the response and recovery effort at a level appropriate for the severity of the Security Incident.

During the investigation of all Security Incidents, the following should be done when appropriate (this will vary with the nature of the Security Incident):

- Determine the nature of the attack or event, point of origin and the intent of the perpetrator(s)

- Identify the systems, processes, and the files affected, or potentially affected, and determine their sensitivity

- Determine if the attack or event was intentional and/or malicious, or whether it was the result of negligence, inadvertence, or some other non-malicious cause

- Determine if the attack or event was specifically directed at Grayson College to acquire specific information or was random

The following section outlines the general process prescribed for assessing security incidents. This is not provided as a step-by-step guide to the definitive tasks to complete in the course of an assessment, but rather as a high-level outline of the processes to follow.

Identify the systems and information affected

Where appropriate, the following information must be determined for all systems affected in each situation:

- IP Address
- Hostname
- Operating System – including patch-level and/or revisions
- Function
- System Operator/Administrator
- Location

NOTE: Machines other than those reported to the IRT may be affected in any given situation and efforts must be undertaken to ensure all relevant hosts are identified and documented.

Also, all information assets affected by the Security Incident must be identified, their sensitivity assessed, (including whether legal consequences are involved, such as breach disclosure requirements or non-compliance with legal or contractual obligations), and their impact on operations, employees, students, and others evaluated.

Identify the aberrant behavior

Aberrant behavior is defined as the root cause of a given situation. The causative behavior may differ from the reported behavior.

Some forms of aberrant behavior may be identified by reviewing and analyzing applicable audit and event log files, including:

- Examining key groups (domain administrators, administrators, etc.) for unauthorized entries in event logs

- Searching for gaps in, or the absence of, system logs on the target system, while comparing systems to previously conducted file/system integrity checks to identify additions, deletions, modifications, and permission and control modifications to the file system and registry

- Reviewing intrusion protection and detection system logs for signs of intrusion, isolating the methods of attack, time and length of attack, and the overall extent of potential damage

- Examining other log files for unusual connections; security audit failures; unusual security audit successes; failed logon attempts; attempts to log on to default accounts; activity

during nonworking hours; file, directory, and share permission changes; and elevated or changed user permissions

- Searching for sensitive data that might have been moved or hidden for future retrieval or modifications

Identify the services/protocols affected

It is important to identify both the services and the protocols affected by the security incident. The services affected are the programs running on a host machine that are being exploited to cause the situation, and/or malware such as cracking utilities, unauthorized processes or other applications running on the compromised systems that are themselves the cause of the Security Incident. The protocols affected are the network communication facilities used to exploit the services.

Example:
In a simple TCP Sync flood attack, the TCP connection queue is filled with requests for service that cannot be fulfilled and therefore will not be removed from the queue until the requests timeout. These requests are made in such duration as to keep the TCP connection queue filled indefinitely. Once the queue is filled the host is unable to respond to further TCP requests. In this example of a Denial of Service attack, TCP is the affected protocol and all TCP services (HTTP, Telnet, SMTP, FTP, etc...) are the affected services.

Identify the source systems

If the security incident involves an external attack, it is important to attempt to identify the source of the attack. Identification of the source systems can be difficult. However, network protocol analyzers, system log files, firewall logs, or intrusion detection system logs can be useful depending on the type of situation. In the event of Denial of Service attacks or in situations involving technical information gathering, firewall logs, intrusion detection logs, and network protocol analyzers are most useful. For intrusions and compromises, system log files can be an additional resource for identifying source machines. It is critical to the ongoing security of Grayson Colleges information technology infrastructure to identify source hosts that are used to disrupt or harm service. The following information should be gathered on any identified hosts, if possible:

- Hostname
- Domain
- Service provider
- Owner

The following resources can be used to find this information:

- Who is servers – http://www.uwhois.com can be searched to provide the correct ownership and contact information on most Top Level Domains

- IP Address Space - http://www.iana.org/assignments/ipv4-address-space contains a list of worldwide address space owners

Where appropriate, this information can be provided to law enforcement or used to contact the organizations responsible for any given Internet host. Any contact should be made only at the direction of the Grayson College Information Security Officer. This contact can be to provide the organization with information concerning apparent unauthorized use of their Internet hosts or to coordinate response activities.

Identify any external hosts affected by Grayson College hosts

Analysis of the information obtained throughout the response should be made to ascertain whether any hosts external to Grayson College were negatively impacted during the situation.

Example:
*A worm attacks an internal **Grayson College** host via SMTP and then attacks an external host From a **Grayson College** machine.*

Identify any published alerts concerning situation

An inquiry should be made to the following organizations to ascertain whether the behavior observed has been reported and is caused by a known vulnerability or exploit:

- CERT/CC (Carnegie Mellon University) http://www.kb.cert.org/vuls/
- ICAT (National Institute of Standards and Technology) http://icat.nist.gov

These organizations maintain databases of vulnerabilities that can be searched with a variety of criterions including operating system, protocol, and service. Many of the vulnerabilities listed in the databases contain information on how to recover from any attacks and how to protect against future attacks. Additionally, the vendor(s) of the affected machines and/or programs should be contacted to see if they have published any alerts relevant to the situation.

Identify countermeasures to protect systems in the future

Information gleaned throughout the assessment should be used to identify countermeasures to protect Grayson College information technology infrastructure from similar situations in the future. Countermeasures implemented may include:

- Firewall/VPN rule modifications
- Enhanced logging or alerting
- Host-based protection mechanisms
- Host based IDS
- Host based Firewall services
- Automated or manual log file analysis or alerting
- System patches or updates applied
- Re-engineering of network communication services
- Modifying authentication mechanisms
- Changing communication protocols
- Utilizing encryption
- Intrusion Detection System enhancements
- Placement of IDS hosts
- Exploit signature modification
- Revisions to internal policies, processes, or procedures
- Enhancement of employee educations or training

4.4 Evidence-Gathering, Protecting and Preserving

In conjunction with its investigation, the IRT must gather and preserve evidence regarding the Security Incident, such as audit trails, log files, contents of files, etc. Once evidence has been gathered, the evidence must be analyzed to determine the cause of the Security Incident, the vulnerability or vulnerabilities being exploited, how to eliminate these vulnerabilities and/or stop the Security Incident. An assessment must also be made to determine how far the Security Incident has spread, e.g., which systems are involved and the extent to which they were compromised.

The evidence gathering and analysis must be performed in a forensically sound manner. This is especially important if the evidence will later be used in a court of law. Once the evidence is gathered, protecting the evidence is essential. Evidence can be easily contaminated either accidentally or intentionally. When Personally Identifiable information (PII) is compromised during an incident IRT will need to engage specialized technical assistance and advice from a third-party expert to ensure the evidence is gathered and preserved in a forensically sound manner. The next section details this further.

4.5 Technical Investigations

Depending on the nature of the Security Incident and corresponding criticality, the IRT may decide to perform a forensic investigation. A forensic investigation will allow Grayson College to gain a better understanding of the intrusion and the attacker.

A forensic expert should be used when there is a need to extract information from the compromised system(s) without altering the original data, and when it is necessary to ensure the admissibility of evidence. In order to interpret the degree to which malicious activity has occurred and to understand the extent of the incurred damage, the forensic investigation is dependent upon the preservation of the information.

At times, the severity or cause of an incident may prompt Grayson Colleges senior management to seek either criminal prosecution or civil litigation. In this situation, the capabilities of Grayson College employees may not be adequate to appropriately conduct a technical investigation of the Security Incident. In the event that Grayson College discovers Personally Identifiable Information during an incident, an external firm specializing in technical incident response and digital media forensics should be engaged. Such forensic investigation must be performed by a third-party forensic analyst with the appropriate certifications and in a manner that is consistent with industry standards.

4.6 Communications During Response Process

The IRP Plan owner and the Information Security Officer must also determine, with the assistance of the IRT, if communications to senior management, employees, students, any regulatory or law enforcement bodies, or any other third party is required or desirable during the Security Incident response process. All such communications should be handled in accordance with the requirements set forth in **Sections 6** and **7**.

4.7 Incident Response Activity Documentation

Incident response activities must be documented thoroughly. Every command issued on an affected machine must be documented to ensure the integrity of any potential evidence. It is many times impossible to tell the scope, severity, and especially the cause of many incidents. What may at times appear to be a minor issue with a trivial cause may indeed be a significant attack from a threat that requires significant resources to investigate and remediate. This may prompt Grayson Colleges VP of IT to engage the services of a professional incident response and digital forensics firm to support potential litigation. It is extremely important in this type of situation that appropriate documentation is made concerning what activities are conducted in all response activities prior to the engagement of professional forensics investigation personnel. This is crucial to prevent potential evidence from being excluded from any future litigation.

Incident Details and Final Findings Reports (for High Severity (Level 1) Incidents) must also be updated, as appropriate, during the Security Incident response process, and thereafter completed and submitted per the requirements of **Section 8**.

4.8 Recovery Operations

One of the primary purposes of this Plan is to ensure an efficient recovery from Security Incidents. Once the Security Incident is contained and eradicated, the IRT must assist in restoring the systems, files, and other affected elements to normal operation with appropriate security.

Upon completion of the Security Incident response activities, care must be taken to ensure that all affected systems are re-deployed into production in a safe and appropriate manner. The following guidelines are provided as recommendations for best practices.

- Whenever possible, wipe the disks of any affected machines before reinstallation
- Replace disks with new media when wiping is not possible
- Rebuild operating systems and system applications from original manufacturer media
- Restore system data from last known (verifiably) clean backup tapes
- Recreate user accounts based on documented approved user lists
- All restored users must be approved by the system or application owners
- Change all passwords for all users on rebuilt systems
- Review all system configuration parameters and ensure they are configured in accordance with documented and approved Grayson College configuration guidelines
- Coordinate all incident recovery operations with all affected system administration personnel, this is critical to ensure appropriate testing
- Test all systems and applications recovered
- If network devices are affected, ensure that any security specific configuration parameters (firewall rule sets, router logging configurations) are appropriately configured according to documented and approved network configuration guidelines
- Notify all affected users upon approval by the Security Incident Response Plan owner that all recovery operations are complete and that the rebuilt systems have been accepted.

Once the affected systems, files, and/or property have been restored, they should be tested to make sure they are no longer vulnerable to the type of attack or problem that caused the Security Incident. Computer systems should also be tested to ensure they will function correctly when placed back into production or on the network. However, care must be taken to ensure that no relevant evidence is destroyed in the process.

4.9 Incident Response Checklist

An IR Checklist should be used in the event of a security-related incident which will assist in tracking activity and providing a summary report capability. Please refer to the IR Checklist in **Appendix E.**

5 Information Protection

All information pertaining to security incidents, including but not limited to the fact that an Incident occurred and the details regarding the Security Incident, are considered confidential Grayson College information and must be safeguarded against unauthorized access unless and until it is made publicly available by Corporate Communications with the approval of the IRP Plan owner and the Information Security Officer.

All internal communications concerning security incidents must be conducted in an efficient/secure manner and be approved by the Information Security Officer. The following guidelines pertain to all internal communications:

- All employees provided any information regarding a Security Incident must have a legitimate need to know.
- Phone conversations should be protected from unauthorized ambient eavesdropping.
- Number of employees involved should be limited to the lowest number required to respond efficiently and appropriately to the situation.

All external communications must be approved by the Information Security Officer and Grayson College Communications.

Investigations can be compromised through inappropriate disclosure of pertinent information. Investigative information should be shared only with the IRT members involved in response activities, as well as other management personnel whose area of responsibility is relevant to the situation. The IRP Plan owner, at the direction of the Information Security Officer, will manage all information disclosures outside of IRT members.

6 Coordination of Internal Communications

In order to reduce confusion and maximize efficiency during the process of responding to Security Incidents, pre-defined methods of communication have been approved to facilitate internal coordination. The methods of communication are listed below.

6.1 Intra-IRT Communications

A list of IRT members with titles are located in **Appendix B**. Any updates or corrections to that list are maintained by the IRP owner until the IRP is updated. To obtain Team Member telephone numbers and email addresses, please direct all requests to the IRP owner or Grayson College Intranet people directory.

6.2 Notification of Affected Users

The IRT will notify Grayson College authorized users of conditions or situations adversely affecting the information technology infrastructure. These alerts may be in the form of email advisories sent to Grayson College user community or may be posted on Grayson College Intranet. ISO maintains a list of IT Security Managers which would be used to coordinate communication to specific affected users.

During the course of responding to a security incident it may be necessary to advise users of direct threats to Grayson College hosts within their purview. In this situation, the IRT is directed to notify users by phone as soon as possible.

6.3 Notification of Senior Management

Notification of Grayson College Executive management team and Information Security Steering Committee on the details of security incidents will be handled by the IRP Plan owner and the Information Security Officer.

6.4 Internal Communications Template

Please refer to **Appendix G** for an Internal Communications Template.

7 Coordination of External Communications

The IRT must comply with all corporate policies and federal, state, and local laws and regulations concerning reporting security incident related information to external organizations. These organizations include regulatory bodies and law enforcement agencies.

Determining whether and how to communicate information regarding the Security Incident to management, employees, and externally is a very important step in the Security Incident response process. Following a Security Incident, the VSIRT, IRP Plan owner and the Information Security Officer must determine whether Grayson College is required by law, industry regulations or public relations purposes to notify third parties about the Security Incident.

All external communications must be approved by the Information Security Officer and Grayson College Communications. The following guidelines should be used to evaluate situations requiring external coordination.

7.1 Directed to Organizations Targeting Grayson College

If the IRT determines that malicious activity, originating outside of Grayson College, is directed at Grayson College information technology infrastructure, and if the IRT is able to determine the source IP addresses of any such malicious activity directed at Grayson College information technology infrastructure, contact should be made with the responsible authority under the guidance of Office of General Consul and GCPD. Contact information can be determined in the manner described above under the heading *Identify the Source Systems*. Information provided to external organizations targeting Grayson College should be limited to the minimum information that is required to facilitate the response required to halt the malicious activity. Upon coordination with the IRP Plan owner the following information should be provided:

- IP and DNS address of source host(s)
- IP and DNS address of target host(s)
- Service/protocol affected
- Brief description of activity
- Any other relevant information as provided by the Security Incident Response Plan owner

In the event that a security incident has been deemed serious enough to pursue civil litigation and/or criminal prosecution, the Information Security Officer will coordinate any release of information under the guidance of Office of General Consul and GCPD and Grayson College Communications.

7.2 Organizations Targeted from Grayson College Systems

If the IRT determines that malicious activity originating within Grayson College information technology infrastructure is directed at an external organization, the IRT should contact the external organization and provide a description of the activity. Upon coordination with the IRP Plan owner, along with the assistance of the Manager of Infrastructure, the following information should be provided:

- IP and DNS address of source host(s)
- IP and DNS address of target host(s)
- Service/protocol affected
- Brief description of activity
- Any other relevant information as provided by the IRP Plan owner

7.3 Grayson College Technical Service Providers

Several organizations provide technical services to Grayson College, including Internet Service Providers (ISPs) that provide communication links between geographically dispersed facilities. These organizations can be extremely helpful in responding to unauthorized activity originating from outside Grayson College information technology infrastructure. In the event that a security incident requires the assistance of any of Grayson Colleges technical service providers, the IRP Plan owner, along with the assistance of the Information Security Officer will provide guidance on what information to provide and what assistance to request.

7.4 Law Enforcement Agencies

The IRP Plan owner, along with the Information Security Officer, and with assistance from OGC, must determine whether contacting law enforcement is required by law and/or desirable. Law enforcement should generally be contacted when the Security Incident is the result of criminal activity. Contacting law enforcement may also be required under certain circumstances. The IRP Plan owner and the Information Security Officer should advise the IRT when these types of Security Incidents occur.

7.5 The Media

If information concerning security incidents at Grayson College becomes public, various print and/or broadcast media representatives may inquire about the situation. The IRT will release no information concerning Grayson College security incidents to media representatives without direct guidance from the IRP Plan owner, the Information Security Officer, and Office of General Counsel. The IRP Plan owner and the Information Security Officer will coordinate any response to media inquiries through Grayson College Communications.

7.6 Liaison Activity

It is critical that the ISO is aware of, and familiar with, external personnel with whom they may interact during the course of responding to a security incident. This is especially true of the various law enforcement agencies involved with computer crime investigations. It is therefore required that the ISO contact the following organizations and become familiar with the personnel assigned to investigate computer crimes:

- Consultant Firms specializing in forensics or technical investigations
- Local Secret Service and Federal Bureau of Investigation Computer Crime Squad
- Local US Attorney's Office
- Local District Attorney's Office
- Local Police Computer Crime Squad

Designated ISO members must contact these agencies annually to ensure current personnel and contact information. The ISO should also be aware of the policies, processes, and procedures these organizations use throughout the course of their investigations.

7.7 Compliance with Breach Notification Obligations

Most states, and some territories, have breach notification statutes that require notice to residents of these states or territories when certain Personally Identifiable Information (PII) regarding those individuals that is exposed to unauthorized third parties. While the specifics of each of these breach notification statutes vary by jurisdiction, they typically require the entity that maintains such personal information to disclose any security breach to the individuals whose personal information was, or is reasonably believed to have been, acquired or accessed by an unauthorized person. They may also require notice to law enforcement, state or federal agencies, and the media as well.

If PII regarding employees, students or other individuals was, or potentially was, exposed by the Security Incident, the Information Security Officer must determine whether notification is required under applicable breach notification statutes or other federal or state laws or regulations. The HIPPA Privacy Officer and other compliance experts at the Grayson College must also be engaged in this process.

Summary reports of security-related events shall be sent to the Texas Office of the Secretary of State on a monthly basis no later than nine (9) calendar days after the end of the month. Grayson College shall submit summary security incident reports in the current form and manner specified by the Texas Office of the Secretary of State. Supporting vendors or other third parties that report security incident information to Grayson College shall submit such reports to Grayson College in the current form and manner specified by the Texas Office of the Secretary of State, unless otherwise directed by Grayson College.

Depending on the criticality of the incident, it will not always be feasible to gather all the information prior to reporting. In such cases, the IRT should continue to report information to the Texas Office of the Secretary of State as it is collected. The Texas Office of the Secretary of State shall instruct Grayson College as to the manner in which they shall report such information. Grayson College shall ensure that compliant reporting requirements are included in any contract where incident reporting may be necessary.

7.8 External Communications Template

Please refer to **Appendix G** for an External Communications Template.

8 Final Findings Report

At the conclusion of each high-severity (Level 1) security incident, a detailed Final Findings report must be completed by the IRT containing the information set forth on **Appendix F**.

The report must be accepted by the IRP Plan owner and the Information Security Officer and disseminated to all parties identified by the VP of IT as appropriate, keeping with the sensitive nature of the report. The report should follow the internal Grayson College documentation standards as applicable.

APPENDIX A – Grayson Colleges Supporting Security Documents

Grayson Colleges Supporting Security Documents:

- Written Information Security Program, Texas Government Code §2054.133
- Information Handling, Backup and Retention Standard
- Grayson College User Account Policy
- Texas Administrative Code Chapter 202 (TAC§202)
- Federal Information Security Management Act
- 16CFR Part 314, Standards for Safeguarding Customer Information [Section 501(b) of the Gramm-Leach-Bliley Act]
- Payment Card Industry Data Security Standard Requirement 12.9
- Health Insurance Portability and Accountability Act (HIPAA)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC202)
- Texas Administrative Code, Title 1, Subchapter 203
- Texas Administrative Code, Title 1, Subchapter 211
- Texas Government Code, Title 5, Subtitle A, Chapter 552
- Texas Penal Code, Chapter 33, Computer Crimes
- Texas Penal Code, §37.10, Tampering with Governmental Record
- United States Code, Title 18 §1030, Computer Fraud and Related Activity
- Copyright Act of 1976
- Digital Millennium Copyright Act October 20, 1998
- Electronic Communications Privacy Act of 1986
- The Information Resources Management Act (IRM) TGC, Title 10, Subtitle B,2054.075(b)
- Computer Software Rental Amendments Act of 1990
- ISO/IEC 27002:2005 standards
- NIST Special Publication 800-53 & 800-171

APPENDIX B – IRT Current Roster

Please refer to the electronic version of this document for the latest IRT Roster.

Title / Role	Name	Email	Phone
VP of IT			
Incident Response Lead			
Networking Security			
Networking Security			
Infrastructure (Unix)			
Infrastructure (Unix)			
Infrastructure (Windows)			
Infrastructure (Cloud)			
Infrastructure (Cloud)			
Research Export Compliance			
Office of the General Counsel			
Chief Compliance Officer			
Office of the Registrar (FERPA)			
HIPAA Privacy Program			
Risk Management			
Communication			

APPENDIX C – Incident Details Gathering

Incident Details Gathering

All Security Incidents should contain the following basic information (to the extent known):

- Date(s) of incident
- Incident Summary
- Type of Incident
- Severity of Incident
- Affected System
- IP Address
- Hostname
- Function
- Location
- Aberrant behavior
- Point of Contact

APPENDIX D – Security Incident Severity

Level		Event Description	Target Time
One		Data or Potential confidential files being sent to third parties. Threat/Attacks that can cause serious damage to company assets. Continuous events of malicious traffic or attacks are Multiple sites and multiple projects are affected by threat/malware.	* Response Time 15 Mins ** Resolution 1 Hour *** Normal Condition 48 Hours
Two		Threat that may infect common systems or spread via popular application in a certain number of days. Two or more workstations or a specific VLAN is affected by threat/malware. Large events of malicious traffic detected.	* Response Time 30 Mins ** Resolution 2 hours *** Normal Condition 4 Days
Three		Single workstation is compromised. Threat/malware identified but no risky effect on the network. Very low incident/events of malicious traffic are monitored. Threats that are already contained by our current system but still require attention.	* Response Time 1 Hour ** Resolution 24 Hours *** Normal Condition 1 week

Classifications

Incident Severity by Priority Level

Security events are evaluated and rated based upon risk to Grayson Colleges network environment and fall into three categories:

- **Level One (High Risk)** – Personable Identifiable Information (PII) or confidential files being sent to third parties or accessed without authorization. Threat/Attacks that can cause a serious damage to company assets. Continuous events of malicious traffic or Attacks are discovered. The threat/malware affects multiple sites and multiple projects

- **Level Two (Medium Risk) -** Threat that may infect common systems or spread via popular application. The threat/malware affects two or more workstations or a specific VLAN. Large events of malicious traffic detected.

- **Level Three (Low Risk) -** Very low incident/events of malicious traffic are discovered. A threat/malware is identified but has no risky effect on the network. A single workstation is compromised

Level One	Level Two	Level Three
Personally Identifiable Information Compromise	Anomaly in Malware baselines	Scans and Probes
Hacking in Progress	Multiple infected hosts detected on a subnet with the same pattern	Antivirus failed to clean
Unauthorized device on the network	Multiple users affected by spam	Multiple logins from different locations or devices
Unauthorized user on the network	Computer Sabotage and Damage	Excessive access to a malicious website from a single internal source
Rogue wireless access points discovered	Computer Intrusion	User reported spam
Denial of Service	Unauthorized access to server	Single infected machine but non-critical
Multiple infected hosts in a Site with the same pattern	Excessive port blocking attempts from antivirus or other monitoring systems.	Suspicious traffic to known vulnerable host
Multiple projects and sites are affected by threat/malware.	Anomaly in DoS baselines	Contained user script, programs or toolkit
Information Theft or Espionage	Repeat attack from a single source	Outdated Virus Definition
Unauthorized user access to confidential data	Logs deleted from source	Anomaly in suspicious activity baselines
Unauthorized subnet access to confidential data	Anomaly in user access and authentication baselines	Excessive traffic inbound (streaming, web, etc.).
Logging source stopped logging	Accessing a malicious website from multiple internal sources.	SMTP traffic from an unauthorized host
		Excessive SMTP traffic outbound.
		Excessive connections to multiple hosts from a single host.
		Excessive exploit traffic from a single source.
		Excessive exploit traffic to a single destination.

APPENDIX E – Incident Response Checklist

IR Checklist

The following IR Checklist should be used in the event of a security-related incident which will assist in tracking activity and providing a summary report capability.

Incident Tracking Number: _____

Date: **Core Team Member:**

Preparation	
Are all members aware of the Incident Response Plan of the organization?	**YES or NO**
Do all members of the Computer Incident Response Team know whom to contact?	**YES or NO**
Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?	**YES or NO**
Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis?	**YES or NO**
Identification	
Did you document impacted systems?	**YES or NO**
Did you record who reported or discovered the incident?	**YES or NO**
Did you document how was it discovered?	**YES or NO**
Are there any other areas that have been compromised by the incident? If so, have they been documented?	**YES or NO**
Did you document the scope of the impact?	**YES or NO**
Did you document the operations impact?	**YES or NO**
Have the source(s) of the incident been located? If so, have they been documented (where, when, and what are they?)	**YES or NO**
Analysis	
Has there been a Review and Collection on the following for Analysis of Impacted Systems:	**YES or NO**
Containment (Short-term)	
Can the problem be isolated? • If yes, then proceed to isolate the affected systems.	**YES or NO**
Are all affected systems isolated from non-affected systems? If Yes, then continue to the Containment (Long Term) section.	**YES or NO**
If No, then continue to isolate affected systems until short-term containment has been accomplished to prevent the incident from escalating any further.	
Containment (Long-term)	

Can the system be taken offline? If yes, then proceed to the Eradication phase. If No, then proceed with long-term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.	**YES or NO**

System-backup	
Have forensic copies of affected systems been created for further analysis?	**YES or NO**
Have all commands and other documentation since the incident has occurred been kept up to date so far? If no, document all actions taken as soon as possible to ensure all evidence is retained for either prosecution and/or lessons learned.	**YES or NO**
Are the forensic copies stored in a secure location? If Yes, then continue onto the Eradication Section If No, then place the forensic images into a secure location to Prevent accidental damage and/or tampering.	**YES or NO**
Eradication & Recovery	
Can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks? If Yes, then proceed with the countermeasures If No, then please document the reason why?	**YES or NO**
Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks? If No, then please document the explanation.	**YES or NO**

APPENDIX F – Final Findings Report

Final Findings Report

A Final Findings report must be provided *within 10 days* after initial eradication of a High-Severity Security Incident.

The following report content and standards must be followed when completing this report.

Executive Summary:
Narrative description of the Security Incident including:

- What Happened?
- How Discovered?
- Who Reported?
- Impact and Risk to the environment

Background:
Timeline of Activity including:

- High-level Overview of IR activities taken
  - Containment, Eradiation, and Recovery actions taken
- External Coordination made
  - Law Enforcement
  - Other Security Incident or Emergency Response Teams
- Any Security Control Modification made to the environment based on the incident

Analysis and Findings:
Analysis & Findings from forensic tools used during the investigation, including:

- Number of accounts at risk, identify those stored and compromised
- Type of account information at risk
- Identify ALL systems analyzed including:
  - Domain Name System (DNS) names
  - Internet Protocol (IP) addresses
  - Operating System (OS) version
  - Function of system(s)
- Timeframe of compromise
- List any data exported by the intruder
- Established *the source* of the compromise (Root-Cause-Analysis)

Recommendations
Contact(s) at entity and security assessor performing investigation
Post-Incident Activity – Lessons Learned Worksheet

The lessons-learned phase will be conducted immediately after the incident has been eradicated and the system or application is functioning in a normal operations manner. The following questions should be captured in the “Lessons Learned” section of the Incident Response report and assists with identifying root-cause.

Lessons-Learned Worksheet

- **Incident No: _____**
- **Security Incident Type:**

Question	Details
Preparation	
What happened, and at what times?	
Were all of the people necessary to respond to the Security Incident familiar with the IRP Plan?	
Were any actions that required management approval clear to participants throughout the Security Incident?	
Identification & Detection	
How soon after the Security Incident started did the Company detect it?	
Could different technologies or more adequate logging have enabled the Company to detect the Security Incident sooner?	
Analysis & Response	
List all parties involved in responding to the incident	
How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?	
What information was needed sooner?	
Were appropriate resources available to the VSIRT?	
Containment	
How well was the Security Incident contained? Did the available staff have sufficient skills to do an effective job of containment?	

Are there changes that could be made to the environment that would have made containment easier or faster?	
Did the Help Desk, technical staff, and the IRT document all of their activities?	
Eradication and Recovery	
Was the recovery complete – was any data permanently lost?	
Were any steps or actions taken that might have inhibited recovery efforts?	
Post-Incident Activity	
What would the staff and management do differently the next time a similar incident occurs?	
What corrective actions can prevent similar incidents in the future?	
What additional tools and/or resources are needed to detect, analyze, and mitigate future incidents?	

APPENDIX G – Communication Templates

Please note that these templates are provided for a point of reference only and still must be approved by Information Security, Legal, and Risk Assurance departments.

INTERNAL COMMUNICATIONS

The following template is provided in the event that a security incident affects multiple parts of the College, requiring a message to be broadcasted internally.

ACTIVE INCIDENT

CONFIDENTIAL

Dear Users,

We are currently investigating an on-going security-related event. As this is an active and on-going incident, we have partnered with [[forensic provider]] and [law enforcement (if necessary) to conduct a thorough analysis and investigation of the issue.

To stay up to date for the latest information on this active investigation, please refer to [[link]]. Additional updates will be broadcasted as well.

RESOLVED INCIDENT

CONFIDENTIAL

Dear Users,

On [MONTH, DAY, YEAR], we have confirmed a breach to our [[systems]] [[affecting/potentially affecting]] impact to our [[employees/students]] who have used [[our services]] from [time frame of breach]].

We are alerting to let you know after a thorough investigation performed by [[forensic provider]], we are confident that all of our systems are no longer affected by this issue and the proper security mitigation and defenses have been enforced throughout Grayson College

The protection of our [[employees/students]] and their data are very important to us as an organization and for this reason, we have partnered with [[credit monitoring company name]] to offer a year free of identity protection services, including credit monitoring.

To learn more about this identity protection service, or to sign up, please refer to [[insert link here]].

If you have any further questions, please direct your inquiry to: [[POC]]

EXTERNAL COMMUNICATIONS

The following template is provided in the event that a security incident affects students, requiring a message to be broadcasted externally.

ACTIVE INCIDENT

Grayson College is currently investigating an on-going security-related event. As this is an active and on-going incident, we have partnered with [[forensic provider]] and [law enforcement (if necessary) to conduct a thorough analysis and investigation of the issue.

To stay up to date for the latest information on this active investigation, please refer to [[link]].

RESOLVED INCIDENT

On [MONTH, DAY, YEAR], we have confirmed a breach to our [[systems]] [[affecting/potentially affecting]] impact to our students who have used [[our services]] from [time frame of breach]].

We are alerting to let you know after a thorough investigation performed by [[forensic provider]], we are confident that all of our systems are no longer affected by this issue and the proper security mitigation and defenses have been enforced throughout Grayson College.

The protection of our students and their data are very important to us as an organization and for this reason, we have partnered with [[credit monitoring company name]] to offer a year free of identity protection services, including credit monitoring.

To learn more about this identity protection service, or to sign up, please refer to [[insert link here]].

If you have any further questions, please direct your inquiry to: [[POC]]

APPENDIX H –

The Hartford Steam Boiler Inspection and Insurance Company
Email: new_loss@hsb.com
Telephone: 888-472-5677 FAX: 888-329-5677

NOTICE OF LOSS

HSB COVERAGE TYPE

Select from list

LOSS SUBMITTED BY

CARRIER		CURRENT DATE
ADJUSTER/EXAMINER:		CLAIM NUMBER
TELEPHONE NUMBER	CELLULAR NUMBER	ADJUSTER FAX #:
MAILING ADDRESS		DATE LOSS REPORTED TO CARRIE
CENTRAL EMAIL ADDRESS	ADJUSTER /EXAMINER EMAIL ADDRESS	
AGENT NAME	AGENT TELEPHONE NUMBER	AGENT EMAIL ADDRESS
INDEPENDENT ADJUSTER/TPA	TELEPHONE NUMBER	EMAIL ADDRESS

LOSS INFORMATION

INSURED		DATE OF LOSS/ DISCOVERY
MAILING ADDRESS:		EMAIL ADDRESS
LOCATION OF LOSS	AFFECTED INDIVIDUAL / CLAIMANT	
INSURED CONTACT NAME	INSURED TELEPHONE NUMBER	CELLULAR NUMBER

LOSS / CLAIM ESTIMATE

DESCRIPTION OF OCCURRENCE / ALLEGATION

POLICY INFORMATION

POLICY NUMBER	EFFECTIVE DATE	EXPIRATION DATE	DEDUCTIBLE
HSB REINSURED FORM NUMBER AND EDITION	POLICY FORM NUMBER AND EDITION		LIMIT
PROGRAM NAME	WRITING COMPANY / DIVISION		THIRD PARTY COVERAGE ☐ **Yes** ☐ **No**

Please include the policy and form declarations, Accord, Invoices, EEOC / Attorney letters, suit papers and other documentation that constitutes the claim.

** The fields below are required for EPL, MPL and E&O Coverage.*

INCEPTION DATE	COVERAGE IN FORCE ☐ **Yes** ☐ **No**	EXTENDED REPORTING ☐ **Yes** ☐ **No**

COMMENTS

6899-SPL REV 2/16

APPENDIX I – Suggested IRT Training Courses

Computer Emergency Response Team Coordination Center

https://www.cert.org/training/

Software Engineering Institute of Carnegie Mellon University

Managing Security Incident Response Teams (VSIRTs)

http://www.sei.cmu.edu/products/courses/cert/managing-cVSIRTs.html

Provides an overview of issues faced by managers of incident response teams and gives direction on how to improve effectiveness and efficiency.

Overview of Managing Security Incident Response Teams (VSIRTs)

http://www.sei.cmu.edu/products/courses/cert/overview-manage-cVSIRT.html

Condensed version of Managing Security Incident Response Teams, meant to provide personnel who coordinate with incident response teams and activities with a basic understanding of IRTfunctions and issues.

Fundamentals of Incident Handling

http://www.sei.cmu.edu/training/P26.cfm

Provides an overview of incident handling processes, techniques, and methodologies.

Advanced Incident Handling for Technical Staff

http://www.sei.cmu.edu/training/P23B.cfm

Provides technical training to incident response team personnel through practical exercises.

The SANS Institute

https://www.sans.org/

The SANS institute conducts Security conferences throughout the year that provide general security training as well as specialized training organized into divisions of specific subject matter known as Tracks. One of the Tracks, System Investigations Forensics and Response, provides specific instruction on investigating and responding to computer incidents. This Track of instruction is recommended to technical personnel involved in incident response.

InfoSec Institute

https://www.infosecinstitute.com/courses/computer-forensics-boot-camp

This course provides basic instruction on handling and analyzing computer evidence.

Document Acceptance

Name		**Name**	
Title	Information Security Officer	**Title**	
Entity	Grayson College	**Entity**	
Signature		**Signature**	
Date		**Date**	

Name		**Name**	
Title		**Title**	
Entity		**Entity**	
Signature		**Signature**	
Date		**Date**	