Church Educational System
Security Operations Center

Information Security
Major Incident Response

BYU BYU HAWAII BYU IDAHO ENSIGN COLLEGE

Author: John Payne, Chief Information Security Officer
Version: 2.08

Revision Date: 11 February 2026
Original Publication Date: 24 February 2020

Table of Contents

Introduction to the Major Incident Response Plan

Purpose

This incident response plan (IRP) outlines procedures related to a major information security event involving confidential or restricted (sensitive) institutional and personal data maintained in any form by Brigham Young University (BYU), Brigham Young University-Hawaii (BYU-H), Brigham Young University-Idaho (BYU-I), and/or Ensign College (shortened throughout the document as "CES Institutions"). While each information security incident has unique aspects, this plan gives the Incident Response Team (IRT) overall guidelines for its responsibilities and actions.

The incident response process allows the CES Institutions to handle information security incidents in a way that provides several benefits:

- Avoiding or minimizing damage to individuals whose personal information may have been compromised
- Helping the campus communities understand the process involved
- Minimizing the impact of the incident on the confidentiality, integrity, and availability of systems and data
- Meeting legal requirements
- Protecting the reputation of the CES Institutions

Overview

The IRP describes the phases of a major incident response and offers Information Security definitions, campus policies, and sample forms and templates used in the process. The IRP is not a proscriptive step-by-step guide to the major information security incident process but provides the framework for the IRT to work under. Each security incident is unique and the process needs to be adapted to each incident.

A compromise of sensitive data may have associated legal obligations to be reported, even if an unauthorized individual only had access to data. The regulations for reporting are based on the victim's place of residence, and some locales have significant penalties related to a failure to respond in a timely manner. Information security incidents should be reported quickly after discovery to engage the response process.

What is an information security incident?

An information security incident involves:

1. The unauthorized use, disclosure, exfiltration, modification, or destruction of institutional data. The information can be in any form: electronic, print, or other.
2. Violations of the following BYU policies:
    i. University Information Use, Privacy, and Security Policy (https://policy.byu.edu/view/index.php?p=207)
    ii. Appropriate Use of Information Technology Resources Policy (https://policy.byu.edu/view/index.php?p=32)
3. Violations of the following BYU-Hawaii policies:

   i. Data Use, Privacy, and Security Policy (https://policies.byuh.edu/it-resources-information)
   ii. IT Resources Acceptable Use Policy (https://policies.byuh.edu/it-resources-acceptable-use)
4. Violations of the following BYU-Idaho policies:
   i. Technology Use and Security Policy (https://webmailbyui.sharepoint.com/sites/Policies/SitePages/Technology%20Use%20and%20Security.aspx)

Incidents are raised for suspected, attempted, or successful cases of the above.

What classifies as a major incident?

The following conditions will trigger the major incident response plan. After an initial investigation, some incidents may be downgraded, if conditions warrant.

1. Any incident that involves confidential or restricted data (see the CES data classifications at https://cesig.prod.brigham-young.psdops.com/0000017b-2ba5-db91-ad7b-ffaf7c560000/information-classifications will be considered a major incident.
   a. When the data classification for a system is not known (as may be the case for a lost device, for example), the data involved will be assumed to be the confidential classification, until proven otherwise. Confidential and restricted data classifications will be combined and called 'sensitive data' through the rest of this document.
2. Any incident that involves ransomware
3. Any incident that involves HIPAA data
4. Loss of personal information as defined in privacy laws and regulations
5. Any cybersecurity incident that impacts the service availability of the entire campus or large portions therein. (Denial of service attack, ransomware outbreak, etc.)
6. Any information security incident involving campus PCI environments
7. Any incident classified as a major incident by the CES CISO or a campus CIO
8. Any incidents that target high profile individuals
9. Any account compromise impacting a significant number of accounts
10. Any incident that may incur significant financial loss
11. Any incident that includes compromised administrative credentials

Who can report an incident? How is it done?

Anyone (including students, faculty, and staff, as well as those not affiliated with the universities) who believes that an information security incident has or may have occurred, should notify the CES Security Operations Center at **(801) 422-7788**. Questions, concerns, or issues can also be emailed to **cessoc@byu.edu**.

BYU-Hawaii: BYU-Hawaii incidents can also be raised to Darryl Kimak at **(808) 675-3206**.

BYU-Idaho: BYU-Idaho incidents can be raised to the IT Major Incident Manager (MIM) at **(208) 710-0113**.

If for any reason contact cannot be made with the contacts listed above, any member of the campus-specific Incident Response Team can be contacted directly to start the process. (See the "Incident Response Team – People and Roles" section below.)

What should be reported?

Any suspicion of a potential security incident associated with sensitive data types should be reported. (See above) Some examples of potential information security events that should be reported include, but are not limited to:

- Any event where someone has reason to believe that computerized information containing sensitive data has been hacked, stolen, lost, or otherwise compromised.
- Lost or stolen laptops, desktop computers, tablets, phones, disk drives, USB drives, or other personal devices containing sensitive data
- A finding that individuals are accessing sensitive data without a business need to know.
- A finding that unsecure plaintext protocols are being used to send sensitive information outside the institutional environment (e.g., an unencrypted website).
- Any storage media - electronic, paper, or other - with sensitive data not disposed of properly at end of life.
- Sensitive data types delivered to the wrong individual by any electronic or physical means.

Note: The good faith acquisition of sensitive institutional data by employees or agents of the one of the CES Institutions is not an information security incident, provided that the sensitive data is not used for a purpose other than a lawful purpose of the CES Institution and where that data is not likely to result in further unauthorized disclosure. Accidental viewing of sensitive data during one's normal employment activities is not considered a security incident if an individual does nothing with that sensitive data.

What should be done (or not done) after reporting?

When an information security incident, or potential incident, has been discovered, care should be taken to leave the related environment untouched until the incident response team and associated security analysts can assess the situation and where possible create a copy of the environment, to use in their forensics activities. This includes not logging into a system or shutting it down. Systems should not be updated or modified after the discovery until instructed to do so from the incident response team. (Exceptions may be made in the case of ransomware, described below.)

As much information about the incident and environment should be shared as possible. People involved, date and time, systems or environments involved, observations made, and any other relevant information should all be shared with the team investigating the incident.

What should be expected after reporting?

After reporting a security incident, an investigation will determine the extent and nature of the incident, the systems and data at risk, and the likelihood of further damage being done. Electronic systems or media may need to be taken offline to preserve the evidence of the issue or to prevent further data loss, damage, or fraud from occurring. The incident response team will take no system offline without first reviewing the situation with the CISO and CIO. (Exceptions may be made in the case of ransomware, described below.)

IT staff and others who are included as a part of the incident response team will be held by the Office of the General Counsel (OGC) under attorney-client privilege and should limit their discussions about the incident with others.

If the reporting individual does not have a direct relationship with the system or data being investigated, they may not hear about the details of the investigation, the mitigation steps taken, or actions taken as a result of any phase of the incident response.

How should the campus community respond to requests from the CES Security Operations Center?

One of the primary functions of the CES Security Operations Center (CES SOC) is to provide security incident response for all information security incidents that occur on the campuses of BYU, BYU-Hawaii, BYU-Idaho, Ensign College or with any related systems. The CES SOC has implemented security monitoring and other tools that can indicate that a security incident has occurred and may contact anyone affiliated with the universities during their investigation. All students, faculty, and staff should cooperate fully with the CES SOC as they gather information, respond to security incidents, and provide recommendations to improve the security posture of the CES Institutions or portions therein.

Law enforcement involvement

Engagement and interaction with law enforcement regarding information security incidents is rare and should only happen at the direction of the Office of the General Counsel, even if law enforcement officers show up looking for evidence unannounced, have a warrant, or interact in any other way. Contact the incident response team members listed in Appendix 2 as “legal” representatives with any questions or concerns in this area.

If the IRT is concerned that a criminal investigation may be needed for a specific investigation, that concern should be reviewed with the campus IMT (Incident Management Team) liaison and the members of the IRT from the Office of the General Counsel.

The exception to this may be contacting the FBI early in a ransomware incident, as described in the ransomware section below.

Major Incident Response Phases

There are six phases of an information security major incident response:

1. **Discovery** – The discovery of an information security incident can come from end users, system owners, automated detection, or outside entities. This discovery should be reported to the CES SOC at **801-422-7788** or **cessoc@byu.edu**.

   BYU-Hawaii: BYU-Hawaii incidents can also be raised to Darryl Kimak at **(808) 675-3206**.

   BYU-Idaho: BYU-Idaho incidents can be raised to the IT Major Incident Manager (MIM) at **(208) 710-0113**.

2. **Mitigation** – Mitigation steps are taken to prevent further loss of data or damage to information technology systems. This may include removing portions or all of a service or services from the network or taking a service down. Mitigation steps typically run in parallel to the investigation phase. Mitigation steps are decided upon by members of the IRT and the system/application owners, then reviewed by the CISO, CIO, and business unit. Key questions to be answered in this phase include:
   a. Do we need to worry about further data exposure or exfiltration before resolution steps can be decided on and executed?
   b. Should the service be shut down, either partially or fully?
   c. What is the financial or business impact of a service outage?
3. **Investigation** – The investigation phase will involve members of the IRT working with system, application, or data owners. Systems should not be updated or modified after discovery until after the investigation has completed. Key questions to be answered in this phase include:
   a. Has a compromise occurred? What is the scope and severity?
   b. Has sensitive data been exposed and/or exfiltrated?
   c. Has there been a financial loss, theft, or other impact that should be communicated to the institutional fraud process?
   d. Is outside forensics assistance required?
4. **Breach Notification** (when necessary) – Potential and/or required breach notification steps are based on the type and volume of the data exposed or exfiltrated. Not all information security incidents result in breach notification. Decisions about breach notification may include input from the CES CISO, campus CIO, CES CIO, and the Office of the General Counsel for non-regulated data. Key questions to be answered in this phase include:
   a. Are there regulatory requirements that dictate a notification process?
   b. What is the required timeframe for notification?
   c. Does the nature of the breach lend itself to notification outside of any regulatory requirements?
5. **Reporting** – Each major incident results in a report generated by the IRT leader that details financial and risk impacts of the breach, resources affected, timeline and details, etc. This report is generated under the direction of and stored by the Office of the General Counsel and is not for public distribution. A summary report is also generated to be shared with

system/application owners and to be used in campus regulatory reports like the annual FACTA report.

6. **Resolution** – Resolution steps are owned by the group that owns the system, application, or data. Resolution of the issues that were factors in the compromise may continue long after the release of an incident report. Key questions to be answered in this phase include:
    a. (If the service was disabled) What are the conditions that need to be satisfied to bring the system back online?
    b. Do system owners have the knowledge, tools, and time to resolve the identified issues?
    c. Has a timeline been established for resolution?

These phases will be described in more detail below. These descriptions are not meant to be prescriptive or proscriptive but are meant to outline the general objects of each phase of the process. The steps, procedures, tools, and actions taken for a major security incident can vary from incident to incident, depending on the circumstances.

Discovery

Anyone (including students, faculty, and staff, as well as those not affiliated with the universities) who believes that an information security incident has or may have occurred, should notify the CES Security Operations Center at **(801) 422-7788**. Questions, concerns, or issues can also be emailed to **cessoc@byu.edu**.

BYU-Hawaii: BYU-Hawaii incidents can also be raised to Darryl Kimak at **(808) 675-3206**.

BYU-Idaho: BYU-Idaho incidents can be raised to the IT Major Incident Manager (MIM) at **(208) 710-0113**.

If for any reason contact cannot be made with the contacts listed above, any member of the campus specific Incident Response Team can be contacted directly to start the process.

Security analysts in the SOC will perform some initial investigation and data gathering around the potential incident to answer the following questions:

- What is the extent and nature of the incident?
- Is Confidential or Restricted data involved?
    - What is the risk to that data?
    - At initial look, does it appear that any of that data was viewed or exfiltrated by non-authorized individuals?
- Has there been a financial loss, theft, or other impact that should be communicated with the insitutional fraud process?
- Are there initial mitigation steps that need to be taken to contain the incident or attacker and prevent information disclosure?

Care should be taken to avoid disturbing or making updates or modifications to software, data, or equipment involved or suspected of involvement with an information security incident. This includes limiting who logs into a system, working as a group to observe what is happening on a system, and so

forth. The pre-discovery running state of a system or equipment needs to be maintained as much as possible until forensics evidence can be generated. External sources of data like centralized security monitoring and log management tools will be used help determine the answers to the above questions.

If the scope of the incident qualifies for the Major Incident Response process, the security analyst will raise the issue immediately to the IRT leader. The IRT leader reviews the details of the discovery with the CISO, discussing the need to engage the major incident process and any initial mitigation needed. The CISO and IRT leader contact the Office of the General Counsel to indicate the execution of the major incident response and the need to begin privileged communication among IRT members for the incident. The CISO and IRT leader then contact the CIO to notify about the incident and gain approval for initial mitigation steps. The Office of the General Counsel sends an email back to the IRT leader requesting that the incident be investigated, and a report be generated, following the template provided in Appendix 2. (See Example request from OCG regarding security incidents below) That email message should be forwarded to all acting IRT members, the IRT legal representative to the IRT should be copied in all incident correspondence among IRT members, with ATTORNEY-CLIENT COMMUNICATION and PRIVILEGED AND CONFIDENTIAL messages added to the start of these correspondences (email in most cases). This is also the case if external resources are used during the incident response.

Note: If the IRT leader or secondary leader are unavailable or unresponsive, please reach out to the CES CISO to begin the incident response process.

Mitigation

The priority after the discovery of a security incident involving Confidential or Restricted data is to contain the incident. The reasonable integrity, security, and confidentiality of the data must be restored. This may involve disconnecting a service from the campus network, either partially or fully.

Note: During the mitigation stage or early in the investigation phase, the incident response team should be gathered (in person or remote) to pray together to ask for the guidance of the Spirit as they work through the incident process. As the team gets stuck in difficult situations or feels the need, they should consider praying together again to ask for divine help with the incident. When that help comes, we should recognize those times and offer a prayer of thanks for the grace that was shared.

Mitigation steps should be discussed immediately after the discovery of an incident involving Confidential or Restricted data. These steps should be decided upon by the IRT, which at this point in the process should include system administrators, application developers, and customer support representatives who are associated with the impacted systems.

Questions to ask when deciding what mitigation steps to take include:

- Do we need to worry about further data exposure or exfiltration before resolution steps can be decided on and executed?
- Do we need to worry about the spread of an infiltration or threat to other IT systems?
- Should the service be shut down, either partially or fully?
    - Can the system be disconnected from the campus network rather than shutting the system down?

- What is the financial or business impact of a service outage?

Containment authority
When appropriate mitigation steps have been decided upon by the IRT, the IRT leader reviews these with the CISO and campus CIO. No mitigation steps should occur without this conversation occurring first, except in the most extreme cases. If the CISO or campus CIO cannot be reached, the IRT leader makes the call on executing mitigation steps and informs the CISO and campus CIO as soon as possible afterward.

Note: While the SOC Director and CES CISO will make every effort to collaborate with local IT staff and leadership about containment needs during a information security incident, speed is also often a factor to prevent further damage as a result of an attack, in all its many forms. The CES CISO (or in their absence the CES SOC Director) has the authority to decide when to disable an account, isolate a host, or contain a network during an incident even when other executives are not available to participate in that decision.

Care should be taken to avoid disturbing or making updates or modifications to software, data, or equipment involved or suspected of involvement with an information security incident. This includes limiting who logs into a system, partnered review to observe what is happening on a system, and so forth. The pre-discovery running state of a system or equipment needs to be maintained as much as possible until forensics evidence can be generated.

The removal of a system, service, application, or equipment from the network is likely to have impact on end users. The internal communications members of the IRT need to be prepared to know how to communicate with the campus community about the associated outage from the mitigation steps taken. They should be prepared to train call center staff on what should and shouldn't be said when end users or others call in to ask about out of service systems.

BYU: Apart from University Communications, university personnel are not authorized to speak to media personnel or representatives of other outside agencies on behalf of the university. (See the "Media Contact Policy" at https://policy.byu.edu/view/index.php?p=33) All media or public affairs inquiries related to a security incident or an outage associated with the mitigation actions taken related to a security incident should be directed to the office of University Communications at 801-422-4511. Other inquiries can be directed to Risk Management at 801-422-4468 or University Police at 801-422-2222. The IRT members should remain focused on the incident itself, and not feel the need to respond to the public at large.

BYU-Hawaii: Apart from University Communications, university personnel are not authorized to speak to media personnel or representatives of other outside agencies on behalf of the University. (See the "Media Contact" policy at https://policies.byuh.edu/media-contract) All media or public affairs inquiries related to a security incident or an outage associated with the mitigation actions taken related to a security incident should be directed to the office of University Communications at 808-675-3457 or communications@byuh.edu. Other inquiries can be directed to BYU Risk Management at 801-422-4468 (BYU Risk Management supports the BYU-Hawaii campus) or Campus Safety and Security at 808-675-3503 or security@byuh.edu. The IRT

members should remain focused on the incident itself, and not feel the need to respond to the public at large.

BYU-Idaho: Apart from University Relations, university personnel are not authorized to speak to media personnel or representatives of other outside agencies on behalf of the University. (See the "Relationship with the News Media" policy at https://webmailbyui.sharepoint.com/sites/Policies/SitePages/Relationship%20with%20the%20News%20Media.aspx) All media or public affairs inquiries related to a security incident or an outage associated with the mitigation actions taken related to a security incident should be directed to the office of University Relations office at 208-496-2000. Other inquiries can be directed to BYU-Idaho Risk and Safety Management at 208-496-5606 or the office of Public Safety at 208-496-3000. The IRT members should remain focused on the incident itself, and not feel the need to respond to the public at large.

Ensign College: Only the Director of Marketing and Communication or the President's designated spokesman may speak for the college. No employee, volunteer, office, department, program, or unit may communicate with the media … without prior approval and direction of the Marketing and Communications Team. (See the External Communications Policy.)

If mitigation actions were taken, the IRT should help the system owners understand the necessary resolution steps to bring the system back online (see #Resolution below).

Investigation

Security incidents are individualized in their nature, creating a prescriptive list of forensics steps to be used in the investigative process is counterproductive. The IRT leader should review the needs for a specific incident with IT staff and security analysts. IRT security analysts will act using industry best practices and own the responsibility for this step. IT staff and others should cooperate fully as the security analysts perform their forensics investigation.

The IRT will conduct a reasonable and prompt investigation into the information security incident to determine the following:

- Has a compromise occurred, and if so, what is the scope and severity?
- Has Confidential or Restricted data been exposed and/or exfiltrated?
- How did the incident occur?
- Can the individual(s) receiving compromised information be determined?
- When did the incident occur?
    - What does the timeline of events look like from the first intrusion, to discovery of the incident, to mitigation steps taken?
- Has the compromise, data exposure, or other risks to the data or associated system been stopped to the full extent possible?
- What system, process, ownership, or personnel changes are necessary or advisable to help prevent similar incidents in the future?
- Were institutional policies and procedures unknown, ignored, or misunderstood?
- What specific records and individuals were impacted or affected by this incident?

--IMPORTANT--

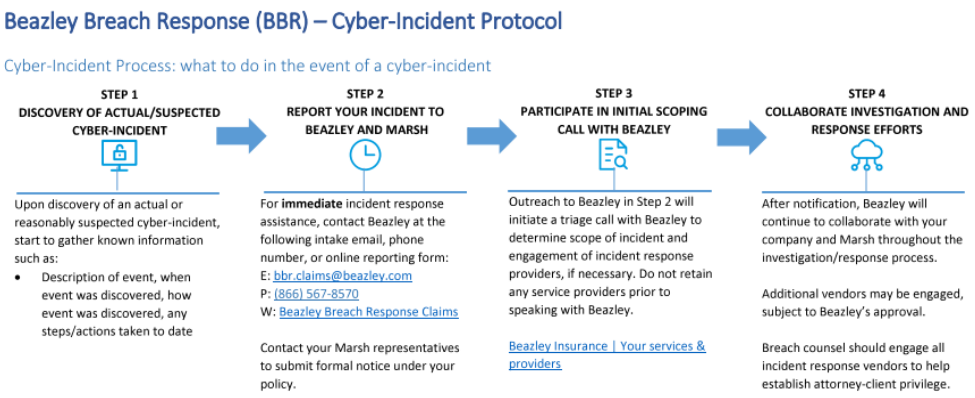
The Falcon Complete team is likely to see and already be working on account or system compromise issues that may raise to the level of a major incident. This may be a decision we make or we may hear the Complete team indicate that an incident has expanded beyond that team's capability or capacity to deal with. They may recommend that we engage with the CrowdStrike IR team via our incident response retainer.

This is a **hard stop point** where we need to call Beazley to **engage our insurer** in the conversation before pulling in more resources. Failure to notify at point will likely result in the insurer rejecting costs for the incident response activities and all related third party legal or breach response needs.

The incident response retainer ensures the CrowdStrike IR team will be the partner selected by Beazley to work with us. We just need to make sure we are being careful about the order of operations being performed. If you have any questions about this, please contact John Payne at 801-592-0098 or Craig Haderlie at 702-245-5756.

External forensics consultants may be used to answer the questions posed for the investigation step. Early in the investigation phase, the IRT should formally discuss the incident, details known, and the ability of the IRT to conduct the investigation in a timely manner. There may be many reasons for external forensics consultants to be used for the investigation phase, including:

- Resource augmentation
  - Investigations requiring more than 150 man hours of work
  - Multiple incidents splitting the availability of the CES SOC
- Incidents of a sensitive nature where a third-party opinion is warranted
- Incidents that are likely to have litigation involved
- Incidents that are likely to have extensive breach notification needs



The IRT leader and CES CISO decide whether to engage with external forensics consultants after consulting with the IRT. If external forensics is needed, the IRT leader will work with BYU Risk

Management to start a claim and get an external forensics partner engaged. It will take some time for an external forensics firm to be selected (this should be CrowdStrike based on the IR retainer we currently carry), the initial scoping call to complete, and an engagement to start. The CES Security Operations Center is generally not in control of the timeline once an external forensics consultant is engaged.

Forensics evidence is likely to be collected by the security analysts during the investigation phase. All evidence collected will be recorded and tracked with an evidence chain of custody tracking form. (See #Evidence Chain of Custody Tracking Form in Appendix 2) At the end of the investigation, this data is stored by the CES SOC, under the direction of the Office of the General Counsel. Retention of data collected for security incidents is set at six years or the end of any corresponding litigation matters, whichever comes last. Please see the Legal and Litigation Hold section below for details about determining what needs to be collected.

The IRT should only communicate findings and progress among team members (remembering that specific departmental IT staff are IRT members for specific incidents). All electronic communication regarding the incident should be made to counsel's attention, marked as privileged and confidential.

Breach Notification

Not all major security incidents result in data breaches. Not all data breaches involve notice triggering information. This phase of the process may not be necessary. Questions about whether breach notification is necessary, from IRT members or others, should be directed to the Office of the General Counsel.

Breach notification is necessary when an incident results in data being exposed or exfiltrated and there are associated legal or regulatory requirements or may happen at the discretion of the IRT.

Non-regulated data

The IRT should help a department understand why it may want to communicate a breach notification for non-regulated data. In general, the approach to date has been to not disclose a notification when there is not an associated regulation that spells out the need for the notification, but there have been exceptions. This should be addressed on a case-by-case basis. Questions should be referred to the member of the IRT from the Office of the General Counsel.

Regulated data

Breach notification for regulated data typically has specific timelines, people and organizations to notify, and is based on the state or country of residence for affected end users whose data was compromised. The Office of the General Counsel and any external breach notification partners (which are members of the IRT) that have been brought in through the cybersecurity insurance company can help with understanding these requirements and timelines.

As soon as regulated data (which typically has the restricted classification) has been found to have been involved in the security incident, the IRT should meet together to discuss the type of data, the volume of

data, and the potential needs if breach notification becomes necessary. Data stewards and appropriate campus compliance leaders should also be involved in this discussion. The IRT leader schedules this meeting. This initial review likely will happen while the investigation phase is ongoing.

The IRT should prepare a notification plan, draft communication for end users, and create relevant timelines. The IRT leader then reviews this with the CES CISO. The IRT leader and CES CISO then decide how to review the breach notification plan with appropriate vice presidents, institutional communications teams, and the campus CIO. No end user breach notification should be released until these reviews are completed.

Method of notification

Notification to affected persons must be provided by one of the following methods unless substitute notification is permitted: written notification by first-class mail to the most recent address the institution has for the individual; electronic notification if the primary method of communication with the person is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001; telephonic notification provided that contact is made directly with the affected persons; or by publishing notice of the breach of system security in a newspaper of general circulation. As appropriate, the CES Institution may issue a press release to the media and conspicuously post on the campus website an "Information Security Incident Notice."

Notification response

Following the release of breach notification of any type, the CES Institutions can expect several inquiries from notified users, their parents/spouses, and security vendors. The IRT should provide any call center listed in the notification with a written inquiry response guide to be used to respond to inquiries by any method.

Note: A number of third-parties provide notification and call center services at a reasonable rate. These services can be accessed via the cyber insurance policy. If email about an incident is sent from one of the campuses and an email address is used that either is brand new or doesn't normally send a volume of email, an email warmup process should be used to ensure that the sent message isn't blocked by email filtering systems.

Reporting

Each information security major incident will be documented in an incident report. The IRT leader writes the report under the direction of the Office of the General Counsel. There are two versions of this report created:

1. An incident report is used to communicate the basic details of the incident with internal need to know individuals

2. An extended incident report, delivered to and stored by the Office of the General Counsel

These reports are related to each other and detailed below. Templates for these reports are located at https://byu.app.box.com/folder/90182482993.

Incident Report

The incident report contains the following:

- Quick Facts – an incident executive summary providing a one-page summary of the incident, resources involved, impacts, risk classification, and reporting information. (See #Quick Facts in Appendix 2)
- Incident Overview – a summary of the incident containing the who, what, when, and where of the incident without providing the specific details outlined in the extended report
- Mitigation Response – a summary of the immediate steps taken to prevent or mitigate damage or further impact
- Incident Impact – a description of the impact to the CES Institution in terms of disruption (time and effort to respond, investigate, and recover), financial loss, reputation/publicity, etc
- Conclusion – a short description of the root cause(s) and/or conditions that enabled the compromise, a description of the type of information and data classification involved, and a determination whether a data breach occurred.

This document is stored by the CES SOC and shared with institutional personnel and committees who have a business need to know regarding security incidents on campus. Examples include:

- Information Security and Privacy Committee (ISPC)
- Executive Risk Management and Compliance Committee (ERMCC)
- FACTA officer

The document is considered confidential and should contain both a watermark and a footer indicating such.

Extended Incident Report

The extended incident report contains everything included in the incident report, as well as the following:

- Remediation recommendations – improvements that can be made to reduce the risk of similar incidents in the future
- A list of individuals who were a part of the incident response team
- A list of management and other staff that were notified of the incident or given updates during the investigation
- A record of evidence collected and stored – a brief description of all forensics evidence collected, the disposition of the forensics evidence, and the retention needs for the evidence.
- One or more appendices, detailing the following, where applicable:
    - Incident details and timeline
        - Details about the attack, if known
        - Detailed report of actions and activities for all phases of the security incident
        - Resolution phase may include ongoing efforts where completion dates are not known.
    - Technical analysis

        - Systems and artifacts analyzed
        - People interviewed
        - Description of methods used and findings/conclusions
    - External forensics findings (when used)
    - External forensics remediation recommendations (when given)
    - Breach notification actions (if applicable)
    - Other details, as needed

This document is stored by the Office of the General Counsel, and requests for access to this document should be directed there. The following individuals outside the Office of the General Counsel also have access to these documents:

- Campus Chief Information Officer
- CES Chief Information Officer (if different from above)
- CES Chief Information Security Officer
- Managing Director, Risk Management and Safety
- Director, CES Security Operations Center
- CES Chief Privacy Officer

The document is considered privileged and confidential and should contain both a watermark and a footer indicating such.

Threat Intel sharing

The CES SOC will block and create alerts for known threats at all four campuses. As appropriate, the SOC will share minimal, non-identifying threat data to external threat intel feeds. The format of this data will be as follows:

- Attacker IP address(es) or email address(es)
- Approximate date and time of attack
- Attack type

Attacker IP or email	Approximate date and time	Attack type
112.245.146.137	10:37 UTC 13 Jan 2020	WebShell deployment – ChinaChopper
91.126.49.219	16:28 UTC 15 Jan 2020	Successful foreign SSH login – brute force
James.smith@gmail.com	03:12 UTC 18 Jan 2020	Phishing email – credential harvesting attempt
Joe.student137@gmail.com	21:02 UTC 19 Jan 2020	Phishing email – gift card scam

Threat intel will be shared with the Church ICS Security Operations Center early in the incident process and throughout the investigation of an incident, to validate that the incident has not extended to church systems or BYU-Pathway.

Resolution

The resolution phase of a security incident involves taking care of factors that lead to the compromise. Resolution steps are owned by the group that owns the system or application and may continue long after the release of the incident report.

Some of the resolution items may be prescriptive, defined by the IRT as conditions that need to be satisfied to bring the system back online. When these have been identified by the IRT, a review should be done with the system owners to ensure they have the knowledge, tools, and time to resolve the identified issues. If system owners are incapable of resolving the issues, external consulting assistance may be required.

In many cases, existing systems may need to be rebuilt, migrated to fresh systems, or otherwise moved when the full integrity of the existing system cannot be established or restored. For ransomware incidents, the system rebuild is a mandatory step.

Business needs may require specific timelines be established for resolution of these issues to restore services. These needs should not pressure the IRT to restore services before required resolutions steps are implemented if sensitive data remains at risk.

Incident Communications

There are a number of different groups that have communication needs during an incident:

- Direct IRT – Those working directly as members of the incident response team
- Indirect IT – IT staff that aren't directly working on the incident, but may have IRT work being displayed, see something that is happening to the side, or have other questions about the security incident that they discover as a part of their normal daily work.
- Campus and CES Executives
- General campus community
- Press and Others
- Law Enforcement
- Notice Obligations – both to government agencies and to individuals

Out of band communication for direct IRT members:

If the nature of the incident is such that there is a suspicion that an attacker has gained control of all or part of a communication tools (like Exchange, Zoom, or Teams), those tools should not be used during incident response activities. We will move to the Cygnvs platform, which is provided by our cyber insurer, Beazley. The existing tenant is normally limited, but if needed during an incident, Beazley will extend access to the entire direct IRT. If that occurs, all communication should happen in the Cygnvs tool. John Payne, Kaylee Hill, and William Jackson have persistent accounts in the tool and can guide the group through the process when necessary. If we need to use the tool, we should **cover that need** during the initial **scoping call with Beazley**. We have only pivoted to out of band communications in a single major incident since 2019, we don't expect to need to pivot to Cygnvs for most major incidents.

The removal of a system, service, application, or equipment from the network is likely to impact end users. The internal communications members of the IRT need to be prepared to know how to communicate with the campus community about the associated outage from the moment mitigation steps taken. They should be prepared to train call center staff on what should and shouldn't be said when end users or others call in to ask about out of service systems.

BYU: Apart from University Communications, university personnel are not authorized to speak to media personnel or representatives of other outside agencies on behalf of the university. (See the "Media Contact Policy" at https://policy.byu.edu/view/index.php?p=33) All media or public affairs inquiries related to a security incident or an outage associated with the mitigation actions taken related to a security incident should be directed to the office of University Communications at 801-422-4511. Other inquiries can be directed to Risk Management at 801-422-4468 or University Police at 801-422-2222. The IRT members should remain focused on the incident itself, and not feel the need to respond to the public at large.

BYU-Hawaii: Apart from University Communications, university personnel are not authorized to speak to media personnel or representatives of other outside agencies on behalf of the University. (See the "Media Contact" policy at https://policies.byuh.edu/media-contract) All media or public affairs inquiries related to a security incident or an outage associated with the mitigation actions taken related to a security incident should be directed to the office of University Communications at 808-675-3457 or communications@byuh.edu. Other inquiries can be directed to BYU Risk Management at 801-422-4468 (BYU Risk Management supports the BYU-Hawaii campus) or Campus Safety and Security at 808-675-3503 or security@byuh.edu. The IRT members should remain focused on the incident itself, and not feel the need to respond to the public at large.

BYU-Idaho: Apart from University Relations, university personnel are not authorized to speak to media personnel or representatives of other outside agencies on behalf of the University. (See the "Relationship with the News Media" policy at https://webmailbyui.sharepoint.com/sites/Policies/SitePages/Relationship%20with%20the%20News%20Media.aspx) All media or public affairs inquiries related to a security incident or an outage associated with the mitigation actions taken related to a security incident should be directed to the office of University Relations office at 208-496-2000. Other inquiries can be directed to BYU-Idaho Risk Management at 208-496-5606 or the office of Public Safety at 208-496-3000. The IRT members should remain focused on the incident itself, and not feel the need to respond to the public at large.

Ensign College: Only the Director of Marketing and Communication or the President's designated spokesman may speak for the college. No employee, volunteer, office, department, program, or unit may communicate with the media … without prior approval and direction of the Marketing and Communications Team. (See the External Communications Policy.)

Direct IRT communications

The incident response team is brought under client-attorney privilege early in the incident process. They should feel free to communicate openly with each other about the incident. As others are brought into the incident response team, they should also be brought under the same privilege and can have full access to the details of the incident.

If individuals need to work together in person, they need to be housed in a workspace that can be protected from having incident details overheard by those that are not under privilege. This may be a conference room with closed doors, the physical area of the Security Operations Center itself, a Zoom or Teams meeting that is not recorded, etc.

If there is any suspicion that a related email system or email account may be compromised, the IRT should not use that email system or account to communicate about the incident. External temporary email accounts may be used, these accounts should be newly set up for use in the incident only, and not be a reuse of an existing personal email account.

Communication with IT staff not directly involved in incident response

IT staff who are not directly involved in the incident response team may see that an issue is happening, especially as systems are taken offline and integrations break. They may not understand the true nature of the issue and both have a desire to help resolve the incident and have a natural tendency to speculate about what really is happening when details are not obvious. Depending on the nature of the associated outage, the campus CIO may have a need to share some incident details without sharing specifics with the IT staff who are not directly part of the IRT.

This communication should help address speculation that may be happening, share the need to follow the process, and potentially bring the entire group under privilege, if necessary. Non-IRT IT staff may need to be reminded of how the information security major incident process works, expected outage windows, and how they can be expected to help.

Communication with campus executives and others

Campus executives and individuals in the CES commissioner's office will likely need both an initial review of the state of the incident, the impacted campus systems, and estimates around how long those systems may be offline. The CES CISO, campus CIO, and CES CIO own the responsibility for sharing those initial and ongoing updates. Some incident details may be shared without sharing specifics, without bringing those groups specifically into client-attorney privilege.

Communication to the general campus community

Information security major incidents often involve critical IT systems being taken offline. When this happens, the campus community immediately notices and begins asking questions about the outages. The process for IT support staff to communicate that an outage is happening should follow the regular process used for any other IT outage. Details do not need to be shared and the language does not need to indicate that an information security incident is occurring. If the normal response in a major incident is to say:

> "We are aware of the issue. Engineers are working to investigate and restore the service. The next update will be given in XX hours."

the same pattern should be followed for major information security incidents.

Some outages may extend for days or weeks. IT support staff should be ready to continue to share approved messaging about an incident until intitutional leadership, working with the IRT, decides to change the messaging about an incident.

If the campus community needs to perform actions, like a mass password reset, a careful review of what is being shared about the incident needs to be done as the request for action goes out. In many cases, the campus community can be asked to take actions like a password reset without giving any details about the security incident itself.

Interactions with the press and other related public entities or individuals

Each CES Institution has an office that is responsible for interacting with media on issues affecting the insititution. The IRT should not feel compelled in any way to respond directly to media requests and should refer those requests to the IRT member from the insitutional office listed below.

Details about information security incidents do not need to be shared with media. The IRT should not share incidents details with individuals, the public, or family. Those details are protected under client-attorney privilege.

Communication with Law Enforcement

All communication or other engagement with law enforcement regarding information security incidents should only happen under the direction of the Office of the General Counsel. This is the case even if law enforcement officers show up looking for evidence or information unannounced, have a warrant, or interact in any other way. The involvement of law enforcement in information security incidents should be rare, except for ransomware incidents, where the IRT needs to work with the FBI early in the process.

Communication as a result of notice obligations

The nature of some information security incidents may warrant the need to communicate the state of the incident with the Department of Education and others early in the Discovery/Investigation phases of the incident as well as periodic updates as the incident response progresses. The Office of the General Counsel owns the responsibility to know when this type of notification is needed, how to communicate this notification, and owns the notification. They may involve third party legal assistance in the process.

If a data breach has occurred (see above) and notice triggering information has been lost, the IRT should provide all necessary information to the Office of the General Counsel. The Office of the General Counsel and institutional communications team should work together to understand the timeframe requirements for breach notifications and to determine the method for providing that notification. They may involve third party legal assistance in the process.

Legal and Litigation Hold considerations

Litigation related to information security incidents is rare, but occasionally happens. For this reason, it is important to avoid destroying anything related to the incident that may later be needed as evidence. This includes but is not limited to systems (or copies of systems), hard drives (or copies of drives), email, and other artifacts. Needs vary from incident to incident; the Office of the General Counsel will provide details on what needs to be preserved and what can be destroyed.

Before the end of the investigation stage of an incident, the IRT should meet to discuss associated incident artifacts, briefing the IRT members from the Office of the General Counsel on what can be preserved. The Office of the General Counsel will create a preservation notice requesting the collection and preserving of specific artifacts. This preservation notice will then be shared with the IRT.

The SOC staff has the responsibility and training to properly collect and store forensics evidence, that work may start early in the investigation phase of the incident. All evidence collected will be recorded and tracked with an evidence chain of custody tracking form. (See #Evidence Chain of Custody Tracking Form in Appendix 2) At the end of the investigation, this data is stored by the CES SOC. Retention of data collected for security incidents is set at six years or the end of any corresponding litigation matters, whichever comes last.

Ransomware Incidents

The detonation of ransomware in the campus environment is a special case that is treated slightly differently than other security incidents. Systems impacted by a ransomware detonation will be taken offline and will not be brought back online: a system reinstall and restore from backup are required. This may result in an extended outage for critical IT systems as recovery steps are taken.

It is critical that any ransomware event (large or small) be brought to the attention of CES SOC immediately. No negotiation or communication should be made by individuals to the attackers. For a ransomware event, the incident response team will engage with ransomware negotiator specialists via the cyber insurance policy.

The steps followed for ransomware are similar to those that are described in the CISA Ransomware Guide, found at: https://www.cisa.gov/stopransomware/ransomware-guide

How to recognize ransomware

The first indication that ransomware has detonated for a server environment is that services have failed. Workstations will have indicators on their desktop that encryption has occurred. Files will be encrypted, usually ending in new extension names, for example “filename.ryuk”

A ransom note is typically left behind sometimes as a popup window, sometimes in addition to a popup window talking about the encryption.

Systems infected with ransomware typically also attempt to infect others on the campus network. The SOC may have indicators that this type of lateral movement is occurring.

Initial immediate containment steps to take

Speed of response is critical in order to contain the spread of ransomware once it detonates. Attackers are very good at spreading quickly through an environment once a foothold has been established. A quick determination of systems impacted needs to be made, immediately removing them from the campus network (disable WiFi, remove ethernet connection, disable vNIC, etc). Systems should be shut down only if they can not be isolated from the campus network in any other way. A running system with an

active ransomware infection can provide valuable information about the attack, powering off the system destroys some of that information.

Contact the CES Security Operations Center at 801-422-7788 immediately. If no answer, contact Kaylee Hill at 360-362-9541 or John Payne at 801-592-0098. If still unable to reach anyone, immediately start calling other IRT members listed in Appendix 2. The CES SOC will quickly need the systems involved (hostname, MAC address, and/or IP address), the estimated scope of the ransomware detonation, and any other containment steps that have been taken.

Investigation

The IRT should not use work email systems/accounts to communicate during the incident until the integrity of the email systems can be confirmed. Individuals will be asked to create new temporary email accounts for use during early stages of the investigation.

For all ransomware events that have spread from one system to another, a third-party forensics firm will be used to help verify containment.

The CES SOC will create a system image and memory capture of one or more impacted systems. This will be used to attempt to gain access to the encryption key used by the ransomware. If the encryption key can be accessed, data may be able to be recovered from a compromised system. A copy (or screenshot) of the ransom note and possibly the memory capture will be shared with the FBI. This will be compared to their documentation to see if they have decryption keys available for the specific ransomware used. Providing the memory capture may allow the FBI to gain access to a new encryption key if they do not already have access to the variant in use.

The IRT will then work to validate that full containment of the ransomware detonation has occurred, how the initial compromise occurred, and recommend changes to be made to prevent a repeat. This will take some time, possibly extending weeks or months, depending on the damage done and number of systems impacted. The standard major incident process detailed above will be used to accomplish these goals.

Some ransomware infections attempt to take the data found on infected systems; others simply encrypt those systems. The ransom note may indicate that data taken is at risk of being posted online. If possible, the IRT should take every effort to discover whether sensitive institutional data was taken. An enumeration of what was taken, the likelihood of the data being exposed publicly, and any other risks or impacts should be shared with institutional leadership.

Recovery

All systems impacted by ransomware require reinstall and restore from backup, from a backup set prior to the detonation of the ransomware. It is not appropriate to place a system infected with ransomware back on the campus network where the ransomware can continue to spread. The compromised system should be considered lost. Backup

systems and associated data should be verified as being clean of ransomware infection before being used.

Recovery should be prioritized, based on the criticality of impacted services. Recovery should not start if initial detection vectors have not been discovered, containment has not been verified, or otherwise given the go ahead from the IRT team. The campus will experience an outage as a result of the incident, that outage will last as long it takes the team to restore the compromised systems.

A password reset of all user accounts is a likely step in the recovery process

Other considerations during a ransomware incident

The CES institutions will not pay ransoms associated with a ransomware infection. Paying a ransom does not guarantee systems will be recovered properly.

Process improvement, feedback, and training

Individuals who have suggestions for improvement, comments, or questions about this process should direct that feedback to the incident response team leader. Anyone (including students, faculty, and staff, as well as those not affiliated with the CES Institutions) can make process improvement suggestions. The IRT leader will review those with IRT members to decide whether to adopt those changes.

At the end of every major incident, the IRT leader should inquire of the team about lessons learned, ways the process could be improved, and who feels like they need additional training in their IRT roles. The lessons learned activity should occur within two weeks of the completion of the investigation phase or the release of notification letters.

If the major incident response process has not been used for a year, the IRT leader should schedule a meeting with IRT members to have them review the IRP, review their roles on the IRT, and address any questions they may have about those roles.

Appendix 1 – Definitions and Policies

Data classification – The CES Institutions classify information assets in order to determine who is allowed to access that information and to understand what security precautions must be taken to protect that information from unauthorized use. This classification also informs the security incident process. The CES data classification guidelines can be found at https://cesig.prod.brigham-young.psdops.com/0000017b-2ba5-db91-ad7b-ffaf7c560000/information-classifications. Systems that contain data which has not been classified or have unknown data residing therein are assumed to be "confidential" until shown otherwise and may start in the major security incident process.

Personal data stored on campus resources by an individual (for example using campus email system for personal uses like taxes) do not come under these classification guidelines, and the CES Institutions are not liable for exposure of that data.

Regulated Data - Types of regulated data include, but are not limited to:

> **Personally Identifiable Information (PII)** - PII is confidential information and includes an individual's first name and last name or first initial and last name in combination with one or more of the following data elements that relate to such individual (depending on the State(s) statute(s) at issue): Social Security number; driver's license number or state-issued identification card number; financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to an individual's financial account; passport number; medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional or health insurance information; or username or email address coupled with a password or security question and answer that would permit access to an online account.
>
> **Protected Health Information (PHI)** - PHI is confidential information and includes information that is created, received, and/or maintained by the organization related to an individual's health care (or payment related to health care) that directly or indirectly identifies the individual.
>
> **Personal Information (Privacy standards)** – The term "personal information" may be used where information is subject to data privacy laws and regulations. This is normally defined as any information that can be used to identify a living, human individual. See the CES data classification guidelines listed above for examples and use cases.

Appendix 2 – Major Information Security Incident Response Teams

Incident Response Team - Core

The Incident Response Team (IRT) may be made up of a number of people across the university or college, as circumstances warrant. The following is a list of individuals who have primary responsibility for functions the IRT may need. Each campus has additional members of the incident response team, brought in for incidents impacting their campus. Those individual team members are listed in subsections following the list of the core IRT team.

An email alias for the core members of the incident response team has been created and will be used for initial incident communications, starting the attorney-client privilege communication, and so forth. The email alias is **infosec-major-incident@byu.edu** and should not be used if there is a suspicion that university email systems or individual accounts of IRT members are compromised.

IRT Leader - Primary		**Office of Information Technology**
Name: **Kaylee Hill**	Title: **Director, CES Security Operations Center**	
Cell: **360-362-9541**	Office Phone: **801-422-6961**	Email: **Kaylee.Hill@byu.edu**
IRT Role: Manages and coordinates the overall response efforts and IRT. Decision maker on utilization of external forensics partners, in conjunction with the CISO. Identifies key tasks, manage timelines and document all response efforts from beginning to end. Summarize the steps needed to assess the scope of a breach. Ensures contact lists remain up to date and IRT members remain ready to respond. Analyzes response efforts post-incident to better prepare the organization and IRT for the next incident.		

IRT Leader - Secondary		**Office of Information Technology**
Name: **Willliam Jackson**	Title: **Lead Security Analyst**	
Cell: **208-818-3170**	Office Phone: **801-422-0026**	Email: **William_Jackson@byu.edu**
IRT Role: Acts as IRT Leader in the absence of the Primary.		

Security Analysts	**Office of Information Technology**
Names: **Eason Taylor** **Anna Pratt** **Matt Mower** **Josh Aughenbaugh**	Title: **Security Analyst**

Cell:	Office Phone: **801-422-7788**	Email: **cessoc@byu.edu**
IRT Role: Participates in discovery, investigation, and mitigation phases of the IRP. Coordinates with University IT organizations to gather needed information, implement mitigation steps, and execute forensics activities to identify compromised data and to determine the when, how, who, and what surrounding the compromise. Maintains integrity of collected forensics data.		

Executive Leader	**Office of Information Technology**	
Name: **John Payne**	Title: **Chief Information Security Officer** **CES CISO**	
Cell: **801-592-0098**	Office Phone: **801-422-9099**	Email: **John_Payne@byu.edu**
IRT Role: Communicates with university upper management about the state of major incidents. Provides executive support for the operation, improvement, and maintenance of the CES SOC. Contributes to the creation, approval, and update of university information security policies and procedures. Final decision on engaging with external forensics partners in conjunction with the IRT Leader.		

Executive Leader	**Office of Information Technology**	
Name: **Brian Radford**	Title: **BYU CIO** **CES CIO**	
Cell: **801-361-4817**	Office Phone:	Email: **Brian_Radford@byu.edu**
IRT Role: Final decision maker on removing university resources from service during an incident. Communicates incident status with university president and CES commissioner. Provides budgetary support for the work of the CES SOC, including resource augmentation needs for incident response.		

Legal - Primary	**Office of the General Counsel**	
Name: **Madelyn Blanchard**	Title: **University Counsel**	
Cell:	Office Phone: **801-422-0469**	Email: **madelyn_blanchard@byu.edu**
IRT Role: Maintains attorney-client privilege during discovery and investigation phases among IRT members. Coordinate with external legal teams as needed. Determines in conjunction with the CISO and CIO whether it is necessary to notify affected individuals, media, law enforcement government agencies, and other third parties, such as card holder issuers. Stores and controls access to extended security incident reports.		

Risk Management - Primary		**BYU Risk Management and Safety**
Name: **Craig Haderlie**	Title:	**Risk Management Director**
Cell: **702-245-5756**	Office Phone: **801-422-2797**	Email: **craig_haderlie@byu.edu**
IRT Role: Understands the insurance and other coverages in place for the University and determines if an incident type is covered therein. Participates in the decision to draw on the external resources that those resources can provide. Acts as a liaison with those resources for the IRT.		

BYU Additional Incident Response Team

The Incident Response Team (IRT) may be made up of a number of people across the university, as circumstances warrant. The following is a list of individuals who have primary responsibility for functions the IRT may need. **Others will also be brought in to participate as needed. IT staff will be incorporated into the incident response team as needed.** IT on the BYU campus is distributed. Incidents will include appropriate IT staff to assist with the incident.

Internal communications - Primary		**Office of Information Technology**
Name: **Brian Anderson**	Title: **Security Training & Communications Manager**	
Cell:	Office Phone: **801-422-0362**	Email: **Briank_anderson@byu.edu**
IRT Role: Internal communications to the campus community, where necessary. External communications (public relations) should be handled through the Campus IMT process. Assists with messaging for the campus community around an incident or associated service interruption. Works with IRT leader, Office of the General Counsel, and IT staff to ensure that messaging doesn't violate attorney/client privilege related to the incident while communicating to end users expected duration of impacts.		

Internal and External communications		**University Communications**
Name: **Natalie Ipson**	Title: **Director, Digital Communications**	
Cell:	Office Phone: **801-422-7302**	Email: **natalie_ipson@byu.edu**
IRT Role: Assists in communications to the campus community. Owns the responsibility for preparing and responding to any external communications needs.		

Campus IMT Liaison		**Risk Management and Safety**
Name: **Tamie Harding**	Title: **Emergency Manager**	
Cell:	Office Phone: **801-422-7881**	Email: **tamie_harding@byu.edu**
IRT Role: Coordinates the emergency management efforts of the Campus Incident Management Team, individuals in the Emergency Coordination Center, the Policy Group, and other organizations, in support of the IRT for all critical cyber incidents on campus. The university Emergency Manager may authorize the use of facilities, equipment, resources, and/or expertise to expedite the response from both within and outside the university.		

BYU-Hawaii Additional Incident Response Team

Executive Leader		**Office of Information Technology**
Name: **Ryan Carter**	Title: **Chief Information Officer**	
Cell:	Office Phone:	Email:
IRT Role: Final decision maker on removing university resources from service during an incident. Communicates incident status with university president and other university executives.		

		Office of IT
Name: **Darryl Kimak**	Title: **Product Manager**	
Cell:	Office Phone: **808-675-3206**	Email: **darryl.kimak@byuh.edu**
IRT Role: Informed about all major incidents. Assists in work needed to engage OIT and the rest of the campus, if necessary, in the incident process.		

Legal - Secondary		**Office of the General Counsel**
Name: **Christian Fox**	Title: **University Counsel**	
Cell:	Office Phone: **801-422-8417**	Email: **christian.fox@byu.edu**
IRT Role: Acts in the absence of the Primary.		

Internal and External communications		**University Communications**
Name:	Title: **Director**	
Cell:	Office Phone:	Email:
IRT Role: Assists in communications to the campus community. Owns the responsibility for preparing and responding to any external communications needs.		

Campus IMT Liaison		**Campus Safety and Security**
Name: **Eugenia Soliai**	Title: **Campus Safety and Risk Manager**	
Cell:	Office Phone:	Email:

	808-675-3411	**eugenia.soliai@byuh.edu**
IRT Role: Coordinates the emergency management efforts of the Campus Incident Management Team, individuals in the Emergency Coordination Center, and other organizations, in support of the IRT for all critical cyber incidents on campus. The university Emergency Manager may authorize the use of facilities, equipment, resources, and/or expertise to expedite the response from both within and outside the university.		

		Office of IT
Name: **Arley Enesa**	Title: **Director, Enterprise Information Systems**	
Cell:	Office Phone: **808-675-4524**	Email: **arley.enesa@byuh.edu**
IRT Role: Informed about all major incidents. Brings direct reports onto the IRT as needed. Team has responsibility for operating systems, Active Directory, Exchange, and university applications.		

		Office of IT
Name: **David Te'o**	Title: **Director, IT Infrastructure**	
Cell: **808-590-8491**	Office Phone: **808-675-3968**	Email: **david.teo@byuh.edu**
IRT Role: Informed about all major incidents. Brings direct reports onto the IRT as needed. Team has responsibility for data center, server/storage, virtualization, and Exchange.		

BYU-Idaho Additional Incident Response Team

Major Incident Manager		**Information Technology**
Cell: **208-710-0113**	Office Phone:	Email:
IRT Role: Oversight and coordination for the campus IT major incident process. Engages tier 3 support employees to join the IRT and work to resolve the incident.		

Executive Leader		**Information Technology**
Name: **Joe McWilliams**	Title:	**Chief Information Officer**
Cell:	Office Phone: **208-496-7010**	Email: **mcwilliamsj@byui.edu**
IRT Role: Final decision maker on removing university resources from service during an incident. Communicates incident status with university president and other university executives.		

Legal - Secondary		**Office of the General Counsel**
Name: **Josh Figueira**	Title:	**University Counsel**
Cell:	Office Phone: **801-422-2049**	Email: **joshua_figueira@byu.edu**
IRT Role: Acts in the absence of the Primary.		

Risk Management - Primary		**Risk and Safety Management**
Name: **Jason Rammell**	Title:	**Risk Management Coordinator**
Cell:	Office Phone: **208-496-5606**	Email: **rammellj@byui.edu**
IRT Role: Understands the insurance and other coverages in place for the University and determines if an incident type is covered therein. Participates in the decision to draw on the external resources that those resources can provide. Acts as a liaison with those resources for the IRT.		

Ensign College Additional Incident Response Team

Executive Leader		**Information Technology**
Name: **David Paulsen**	Title: **Chief Information Officer**	
Cell: **801-699-0123**	Office Phone:	Email: **david.paulsen@ensign.edu**
IRT Role: Final decision maker on removing college IT resources from service during an incident. Communicates incident status with the college president and other executives.		

Legal - Secondary		**Office of the General Counsel**
Name: **Rich Hatch**	Title: **University Counsel**	
Cell:	Office Phone: **801-422-0982**	Email: **richard_hatch@byu.edu**
IRT Role: Acts in the absence of the Primary.		

Communications		
Name: **Kirk Rawlins**	Title: **Director, Marketing & Communications**	
Cell:	Office Phone: **801-524-1902**	Email: **krawlins@ensign.edu**
IRT Role: Designated individual for all external communications from the College.		

External Resources

The following are external contacts that may be called upon to assist the IRT. The IRT makes the determination when these resources need to be called upon.

		FBI Field Office
Website: https://www.ic3.gov/compliant/default.aspx/	Provo office: **801-374-5332**	24x7 helpdesk: **801-579-1400**
Purpose: Contact for all ransomware incidents. The FBI will report if decryption keys are available. This contact can also be used for law enforcement inquires or needs. The helpdesk can be contacted 24x7, posting incident details on the ic3.gov site will route the details to the appropriate local agent. Create a report on the ic3.gov site first, then call. The Provo office can be contacted during business hours, the helpdesk can be contacted 24x7. An indication that we have a cyber related incident will have the call routed to an appropriate agent.		
Contact/Liaison: **The Office of the General Counsel**		

Utah Cyber Intelligence Analyst		**UTAH SIAC**
Website: https://siac.utah.gov/cyber-crime-tip-form	Phone: **801-965-3838**	Email:
Purpose: Incident intel sharing. The Utah SIAC takes provided intel and shares with applicable parties. Intel should be shared if other organizations in the area may be at risk.		
Contact/Liaison: **IRT leader in conjunction with the Office of the General Counsel**		

Other CES and Church Security Contacts

Name: **Josh Bocchino**	Title: **Manager, ICS Security Operations Center**	
Cell: **360-281-7727**	Office Phone: **801-240-3917**	Email: **joshbocchino@churchofjesuschrist.org**

	Title: **ICS Security Operations Center**	
Cell: **NA**	Office Phone: **801-240-1919**	Email: **secops@churchofjesuschrist.org**

Appendix 3 – Sample Forms and Templates

Quick Facts

The Quick Facts template is used in the incident report as an executive summary for information security major incidents. Details are fleshed out as the incident response stages progress.

Quick Facts		
Date of Incident		
Description		
Financial Impact		
Risk Impact	• High / Medium / Low	
Resource Affected		
Resource Purpose		
Resource Location		
Owner/Contact		
Method Used to Gain Access		
How Discovered		
Information Risk Classification		
FACTA reporting state	**(Reportable/Recordable)**	
Did breach notification take place?		
Did a fraud investigation take place?		
Was law enforcement notified?		

Evidence Chain of Custody Tracking Form

The chain of custody tracking form should be used whenever forensics assets are collected by any member of the incident response team, during any step of the major incident response process. This form is used for tracking and disposition of the evidence collected and becomes an artifact that is attached to the incident record. Any member of the incident response team can and should start a chain of custody tracking form when they are given a forensics object. The form can be found at https://byu.box.com/s/evflugqjltu0v0p1pybs5h1c77lmdo0u

Church Educational System
Security Operations Center

Evidence Chain of Custody Tracking Form
CES Security Operations Center

Incident Number: _____ Incident Name: _____

Submitting Individual Name: _____

Submitting Individual ID #: _____ _____ Signature

Submitting Individual Location

☐ CES SOC ☐ BYU ☐ BYU Hawaii ☐ BYU Idaho ☐ Other: _____

Receiving Individual Name: _____

Receiving Individual ID #: _____ _____ Signature

Date Received: _____ Time Received: _____ Evidence Location: _____

Description of Evidence

Item #	Description of Item (Model, Serial #, Condition, Marks, Scratches)	Comment/Location

Evidence Chain of Custody Tracking Form – CES Security Operations Center

Chain of Custody

Item #	Date/Time	Released by Signature	Released by ID #	Received by Name	Received by Signature	Received by ID #	Reason	Comment/Location

Evidence Chain of Custody Tracking Form – CES Security Operations Center

Example request from OCG regarding security incidents

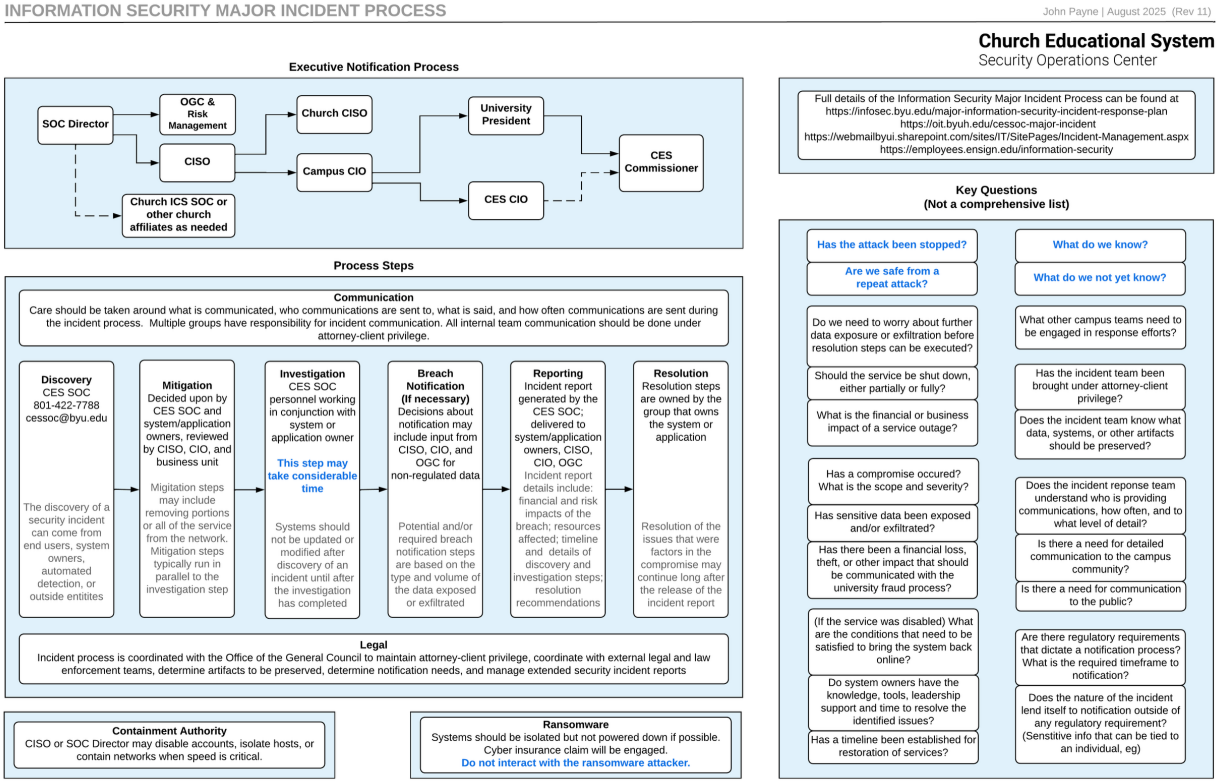
ATTORNEY-CLIENT COMMUNICATION
PRIVILEGED AND CONFIDENTIAL

In response to a recent report {description of the incident circumstances}, the BYU Office of the General Counsel (OGC) (1) has undertaken a privileged and confidential investigation and (2) has been asked to provide legal advice regarding the findings of the investigation.

I am writing to formally memorialize our request for your assistance in this matter in the preservation and analysis of information that may be relevant to this investigation. In assisting in this investigation, you will be acting under the direction of the OGC in providing legal services to the university in this matter. As a reminder, information regarding the investigation of this incident and communications to and from counsel should be kept confidential. Further, neither these communications nor the fact of this investigation should be disclosed to anyone other than university employees with a need to know or others to whom OGC has authorized disclosure.

In addition, the OGC is requesting from you a final report regarding your findings and analysis of {description of the incident circumstances}. This written report should be clearly marked “Privileged and Confidential" and distribution should be carefully restricted.

Appendix 4 – Process Diagram



A copy of this diagram can be found at:
https://infosec.byu.edu/major-information-security-incident-response-diagram
https://byuh.teamdynamix.com/TDClient/1902/Portal/KB/ArticleDet?ID=130771
https://webmailbyui.sharepoint.com/sites/IT/SitePages/Incident-Management.aspx
"Files" section of the 'CES CIO Leadership' Teams channel

Appendix 5 – Change Log

24 February 2020 – Version 2.0

Rewrite of the 2014 version of the university Information Security Incident Response document. Rewrite attempts to be more consumable for end users, align closer with current process, and identify current individuals responsible to act as the Incident Response Team (IRT). It is expected that this document will be updated quickly as roles change going forward, so that it can be used as a guide for all information security major incident response efforts.

9 March 2020 – Version 2.01

Renumbering of Appendices. There were two "Appendix 2" designations, which has been corrected.

11 February 2021 – Version 2.02

Updated IRT members to align with current organizational structures and assignments

Removed vendor section. Has been unused in 18 months, the data keepings changing, and is an incomplete picture of potential vendor contacts.

Added "Any incident that includes compromised administrative credentials" as a criteria defining a major information security incident

Updated Chain of Custody and Incident Process diagrams

Stronger description of threat intel sharing with the Church Security Operations Center

Description of notification to church risk management added

20 Sept 2021 – Version 2.03

Minor grammar and typographical edits

Updated IRT members to align with current organizational structures and assignments

Update to the name of the newly updated campus Information Use, Privacy, and Security Policy

Updated data classification hyperlinks. The term "Highly Confidential" has now been replaced with "Restricted". Description of the details of the data classifications themselves have been removed in favor of pointing the reader to the source documentation for data classification.

Ransomware section added

Incident Communications section added

Incident Process diagram refreshed

14 Oct 2021

Minor grammar and typographical edits

Thanks to Jearlene Leishman and William Jackson for finding the issues in the document.

29 Nov 2021 – Version 2.04

Refactor of document from being BYU specific to covering BYU, BYU-Hawaii, and BYU-Idaho.

13 Jan 2022

Addition of hyperlinks to this document for BYU-Hawaii and BYU-Idaho

5 May 2022 – Version 2.05

Corrected the URL for the BYU-Hawaii IT Resources Acceptable Use policy

Billy Wilson removed, Josh Aughenbaugh added (security analyst)

Will Jackson added as secondary IRT Leader

28 June 2023 – Version 2.06

IRT memberships adjusted for all campuses to reflect current organizational structures.

3 May 2024 – Version 2.07

Replaced university seals with corresponding logos to meet current branding guidelines.

Inclusion of Ensign College in the incident response plan

IRT memberships adjusted to reflect current organizational structures and roles.

11 Feb 2026 – Version 2.08

Updates to the incident process diagram

Added any incident involving ransomware as an input to the process

Added a note about contacting our cyber insurer Beazley before engaging our incident response retainer with CrowdStrike in order to preserve our ability to process incident claims through Beazley

Added a statement about the importance of including prayer as a part of the incident response process.

Out of band communications protocols added.

Incident response team membership updated to reflect current organizational structures

Language about the campus communities avoiding any communication or negotiation with a ransom demand

Formal containment authority to disable an account, isolate a host, or contain a network is clearly defined. (2024 CSMA 5.5)

Lessons learned activity to happen no later than two weeks after the end of an investigation phase or the release of notification letters.