Brigham Young University

Information Security
Major Incident Response

Author: John Payne, Chief Information Security Officer
Version: 2.02

Revision Date: 11 February 2021
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 highly confidential (sensitive) institutional and personal data maintained in any form by Brigham Young University and/or its auxiliary 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 university 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 university community understand the process involved
- Minimizing the impact of the incident on the confidentiality, integrity, and availability of university systems and data
- Meeting legal requirements
- Protecting the reputation of the university

Overview

The IRP describes the phases of a major incident response and offers Information Security definitions, campus policies, and sample forms and templates that are 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 highly confidential 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, 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 university information. The information can be in any form: electronic, print, or other.
2. Violations of the university Information Security and Appropriate Use Policy (https://policy.byu.edu/view/index.php?p=207). This document has been revised, the update is under review and is anticipated to be released in early 2020
3. Violations of the university Appropriate Use of Information Technology Resources Policy (https://policy.byu.edu/view/index.php?p=32)

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 initial investigation, some incidents may be downgraded, if conditions warrant:

1. Any incident that involves confidential or highly confidential university data (see https://infohub.byu.edu/uploads/2016_CES_CIO_Approved_CES_Inform.pdf) 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 highly confidential data classifications will be combined and called 'sensitive data' through the rest of this document.
2. Any incident that involves HIPAA data
3. Loss of personal information as defined in privacy laws and regulations
4. Any cybersecurity incident that impacts the service availability of the entire campus or large portions therein. (Denial of service attack, ransomware outbreak, etc.)
5. Any information security incident involving campus PCI environments
6. Any incident classified as a major incident by the University CISO
7. Any incidents that target high profile individuals
8. Any account compromise impacting a significant number of accounts
9. Any incident that may incur significant financial loss
10. Any incident that includes compromised administrative credentials

Who can report an incident? How is it done?

Anyone (including BYU students, faculty, and staff, as well as those not affiliated with the university) 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**. If for any reason contact cannot be made with the SOC, any member of the 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 university 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 university (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 university data by university employees or agents of the university is not an information security incident, provided that the sensitive data is not used for a purpose other than a lawful purpose of the university 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. Systems should not be updated or modified after the discovery until instructed to do so from the incident response team. This includes not logging into a system or shutting it down.

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 university 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. No system will be taken offline by the incident response team without first reviewing the situation with the University CISO and CIO.

IT staff and others who are included as a part of the incident response team will be held by the university 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 BYU campus or with BYU related systems. The CES SOC has security monitoring and other tools which can indicate that a security incident has occurred and may contact anyone affiliated with the university in the course of their investigation. All BYU

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 university 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 OGC, even if law enforcement officers show up looking for evidence unannounced, have a warrant, or interact in any other way. Contact the members of the incident response team 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 as well as the members of the IRT from the Office of the General Counsel.

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.
2. **Mitigation** – Mitigation steps are taken to prevent further loss of data or damage to University 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 university 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 CISO, CIO, and OGC 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 OGC 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 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 circumstances.

Discovery

Anyone (including BYU students, faculty, and staff, as well as those not affiliated with the university) 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**. If for any reason contact cannot be made with one of these two groups, any member of the 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:

1. What is the extent and nature of the incident?
2. Is Confidential or Highly Confidential data involved?
    a. What is the risk to that data?
    b. At initial look, does it appear that any of that data was viewed or exfiltrated by non-authorized individuals?
3. Has there been a financial loss, theft, or other impact that should be communicated with the university fraud process?
4. 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 OGC 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 Highly Confidential 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.

Mitigation steps should be discussed immediately after the discovery of an incident involving Confidential or Highly Confidential 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 university systems?
- Should the service be shut down, either partially or fully?
    - It is better to disconnect a compromised system or equipment from the campus network, or otherwise isolate the service from end users and the public, rather than shutting systems down?
- What is the financial or business impact of a service outage?

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

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 university 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. This is likely to include call center staff in the Office of IT (OIT) as well as departmental support staff.

Apart from University Communications, university personnel are not authorized to speak on behalf of the university to media personnel or representatives of other outside agencies. 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.

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

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 Highly Confidential 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?

Security incidents are individual 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.

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 CISO decide after consulting with the IRT whether to engage with external forensics consultants. If external forensics consultants are needed, the cybersecurity insurance company will be contacted to engage those third-party services. It may take anywhere from 24 to 72 hours for an external forensics firm to be selected, the initial scoping call to complete, and an engagement to start. BYU is generally not in control of the timeline once an external forensics consultant is engaged.

Church Risk Management will be notified of the security incident by BYU Risk Management. This will allow them to be prepared if the incident extends to other campuses, and further resources are needed to mitigate, investigate, and resolve the incident. Other church schools and environments are not covered by the BYU cybersecurity insurance policy.

The CES SOC will maintain an annual budgetary allotment for external forensics deductibles. This will allow the IRT to move quickly when they believe external assistance is required.

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, in conjunction with University Records Management. Retention of data collected for security incidents is set at six years or the end of any corresponding litigation matters, whichever comes last.

The IRT should take care to 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

Note: 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 OGC.

Breach notification is necessary when an incident resulted 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. The document "Breach notification guidelines for non-regulated data" (currently unpublished) provided by the Office of Information Security should be used as a guide.

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 CES SOC, the OGC, and external breach notification partners (all of which are members of the IRT) that have been brought in through the university cybersecurity insurance company can help with understanding these requirements and timelines.

As soon as regulated data (which typically has the highly confidential 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 university cybersecurity insurance policy includes breach response notification services through contracted, third-party companies. The IRT should discuss whether external notification assistance may become necessary. The cyber security insurance company should be notified early in the process if possible. The CESSOC does not budget funds for breach notification activities, funding to pay for any necessary breach notification needs to be addressed case by case.

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

Example breach notification messages are provided in appendix 2:

- #Example breach notification to BYU users not enrolled in DUO
- #Example breach notification to BYU users enrolled in DUO

These are just listed as examples, content of a notification depends on the type of information lost, and the current applicable laws.

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 university has for the individual; electronic notification if the university's 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 university 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 university 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.

Reporting

Each information security major incident will be documented in an incident report. The report is written by the IRT leader under the direction of the OGC. There are two versions of this report created:

- An incident report used to communicate the basic details of the incident with internal need to know individuals
- An extended incident report, delivered to and stored by the OGC

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 university 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 Office of Information Security and shared with university 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)
- University 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 OGC, and requests for access to this document should be directed there. The following individuals at the University outside the OGC also have access to these documents:

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

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 alert against and block known threats for all three campuses. There are a number of threat intel feeds that the CES SOC consumes from the industry (Ren-ISAC, Stinger (Duke), etc). This threat intel is enhanced when the members that consume the threat intel add to it. As appropriate, the SOC will share minimal, non-identifying threat data back to these 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

Potential audiences for this data may include:

- Church ICS Security Operations Center
- REN-ISAC
- Utah SIAC
- FBI Cyber team

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

Resolution

The resolution phase of a security incident involves taking care of factors in 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.

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.

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 BYU students, faculty, and staff, as well as those not affiliated with the university) 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.

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 university classifies 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 university data classification guidelines can be found at https://infohub.byu.edu/uploads/2016_CES_CIO_Approved_CES_Inform.pdf. There are four data classifications defined in the guidelines, as follows:

Public – information that may be available to the public and has formally been approved for public release. Examples include but are not limited to:

- Course catalog information
- Press releases
- Newletters

Internal – information which is general accessible within the university to those with a legitimate university purpose as allowed by statue, regulations, other legal obligations, mandates, or policy. This information is not intended for entities or persons outside the university. This information is typically not specifically restricted by statue, regulations, or legal obligations. Examples include but are not limited to:

- Student academic records
- Employee personal contact information
- University policies and procedures
- Organization charts

Confidential – information which may not be specifically protected by statue, regulations, or other legal obligations or mandates but is considered by the university's senior management to be private and confidential. Examples include but are not limited to:

- Salary or other personnel data
- Contracts
- Non disclosure agreements with vendors or clients
- Donor contact information

Highly Confidential – information which requires the strictest rules of handling and usage, is protected or regulated by statues, policies, or regulations, or may also include information which an owner has exercised their right to restrict access. Examples include but are not limited to:

- Accounting data and internal financial reports
- Birthdate combined with last four digits of SSN and name
- SSN and name
- Tax ID and name
- Health insurance information
- Medical records
- Bank account or credit card PAN data

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 university is not liable for exposure of that data.

Further questions about data classification can be directed to Brad Stone (University Information Governance) at 801-422-7459 or brad_stone@byu.edu.

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. Examples of personal information include name, BYU ID, email address, direct phone number, home or work address, or any other information that could be used to identify an individual. Some personal information, such as name and email address may be classified as Internal and may be shared with employees and vendors who have a legitimate business purpose for the information. Other personal information may be classified as Confidential or Highly Confidential such as date of birth and religious affiliation.

Appendix 2 – Major Information Security Incident Response Team

People and Roles

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 in OIT will include appropriate IT staff to assist with the incident. Incidents related to departmental systems will involve that department's IT staff.

IRT Leader - Primary		**Office of Information Technology**
Name: **Adam Baker**	Title: **Director, CES Security Operations Center**	
Cell: **910-528-6026**	Office Phone:	Email: **Adam_Baker@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: **Dave Allbee**	Title: **Security Analyst (SME for Incident Investigation and Response)**	
Cell: **801-717-0519**	Office Phone: **801-422-6476**	Email: **kevdave@byu.edu**
IRT Role: Acts as IRT Leader in the absence of the Primary.		

Security Analysts		**Office of Information Technology**
Names: **Mike Watson** **Kaylee Hill** **Dave Allbee** **Nathan Peterson** **William Jackson**	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: **Tracy Flinders**	Title: **Chief Information Officer CES CIO**	
Cell:	Office Phone: **801-422-6101**	Email: **tracyf@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: **Paul Angerhofer**	Title: **University Counsel**	
Cell:	Office Phone: **801-422-6727**	Email: **paul_angerhofer@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.		

Legal - Secondary		**Office of the General Counsel**
Name: **David Andersen**	Title: **University Counsel**	
Cell:	Office Phone: **801-422-6102**	Email: **david_andersen@byu.edu**
IRT Role: Acts in the absence of the Primary.		

Risk Management - Primary		**Risk Management and Safety**
Name: **Branden Wilson**	Title: **Managing Director**	
Cell: **801-360-1819**	Office Phone: **801-422-9016**	Email: **branden_wilson@byu.edu**
IRT Role: Risk Management contact on the IRT.		

Risk Management - Secondary		**Risk Management and Safety**
Name: **Roy Angel**	Title: **Risk Management Director**	
Cell: **801-404-9739**	Office Phone: **801-422-5779**	Email: **roy_angel@byu.edu**
IRT Role: Risk Management contact on the IRT.		

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

Cybersecurity Insurance - Secondary		**Risk Management and Safety**
Name: **Branden Wilson**	Title:	**Managing Director**
Cell: **801-360-1819**	Office Phone: **801-422-9016**	Email: **branden_wilson@byu.edu**
IRT Role: Acts in the absence of the Primary.		

Internal communications - Primary		**Office of Information Technology**
Name: **Brian Anderson**	Title:	**Security Training & Communications Manager**
Cell:	Office Phone: **801-0362**	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, OGC, 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 communications - Secondary		**University Communications**
Name: **Natalie Ipson**	Title:	**Director, Digital Communications**
Cell:	Office Phone: **801-422-7302**	Email: **natalie_ipson@byu.edu**
IRT Role: Acts in the absence of the Primary.		

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.		

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.

Cybersecurity Insurance Company

		Beazley Breach Response Services
Website: **https://www.beazley.com/claims/bbr.html**	Phone: **866-567-8570**	Email: **bbr.claims@beazley.com**
Purpose: Cybersecurity insurance company that can provide the following external services under our contract, with a retention for each: Legal services, Forensics, and Public Relations/Crisis Management Breach response, Credit and identity monitoring, etc. It is preferred that Risk Management maintain this relationship and initiate contact for help for incident response or other services.		
University Contact/Liaison: **Craig Haderlie (Risk Management)**		

CES Security Contacts

Name: **Chaymie Keala**	Title: **BYU–Hawaii IT Security Coordinator**	
Cell:	Office Phone: **808-675-4524**	Email: **chaymie.keala@byuh.edu**

Name:	Title: **BYU–Idaho Major Incident Coordinator**	
Cell:	Office Phone: **208-701-0113**	Email:

Name: **Nick Champlin**	Title: **LDSBC IT Security Specialist**	
Cell:	Office Phone: **801-524-8184**	Email: **nchamplin@ldsbc.edu**

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

Name:	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 breach notification to BYU users not enrolled in DUO

Dear {NAME},

Recently the CES Security Operations Center discovered that some BYU NetIds and passwords on a BYU website may have been exposed, including yours. We do not have any evidence of an unauthorized login using your NetId. For your protection, **your NetID password must be changed before {DATE} or your account will be locked.**

Here are the instructions for a NetID password reset:

Check to see if you can sign in to your BYU Account:

1. Go to my.byu.edu
2. Click *Sign In*
3. Enter your username and password and click *Submit*

If you can sign in:

1. Expand the Miscellaneous drop-down in the *Campus Links* section
2. Select the *Change Password/Security Qs* option
3. Reset Password
4. Add/Update Security Questions
5. Optional: Add DUO Multifactor Authentication (See below for more information)

If you are unable to sign-in, but have security questions:

1. Make sure you are back at the Sign In page
2. Click on the *Password* link in "Forgot your *NetID* or *Password*"
3. Enter your NetID
4. Answer those questions
5. If entered correctly, a temporary password will be emailed to your email account on file.
6. You will use this temporary password at www.byu.edu/password to create a new password.

If you cannot sign into your BYU Account or would like help checking the status of your personal information, please call the *BYU Operations and Support Center (OSC)* at *801-422-4000.*

After changing your password, please take the time to perform the following checks and confirm that your data has not been changed:

1. If you are a current BYU employee and you have a premium email account, verify that you can access your email by logging in.
2. Check the inbox rules to see if there are any suspicious rules.
    a. In Outlook, click "Files", "Manage Rules & Alerts", delete any unwanted rules.
    b. For other providers, search online. For example: "Gmail Rules".
3. Confirm your direct deposit information and other financial information is accurate in My Financial Center.
4. Check that your personal information is accurate.
5. Check other information (i.e. parking registration, e-mail alias manager, etc.)

Enrolling in Duo - We noticed you have not signed up for DUO Multifactor Authentication. DUO is a security system that requires a secondary form of authentication to verify a user's identity and helps protect user's logins. This means that, if a malicious hacker has your password, they will not be able to access your account without access to your device (phone, computer, passcode token, etc.). Please take the time to sign up for DUO to help secure your BYU account and your sensitive information. For more information, please visit duo.byu.edu.

If you have used the same login id and password for other sites and apps, we recommend that you change your password anywhere it's used to protect your accounts from a multitude of online threats. Ideally, you would have different passwords for each account. For more information on how to secure your online presence, visit besafe.byu.edu.

Our security team is actively working to ensure that victims of these compromises are notified and that their accounts are secured. If you have further questions, please contact the BYU Operations and Support Center (OSC) via call or text (801-422-4000), email (it@byu.edu), or chat (it.byu.edu).

Example breach notification to BYU users enrolled in DUO

Dear {NAME},

Recently the CES Security Operations Center discovered that some BYU NetIds and passwords on a BYU website may have been exposed, including yours. We do not have any evidence of an unauthorized login using your NetId. Our records also indicate that you are using DUO. Thank you! Using DUO helps protect you *and* BYU from access by unauthorized users. In response to the possible compromise of your BYU login credentials, we recommend that you reset your NetID password as soon as possible.

Here are the instructions for a NetID password reset:

Check to see if you can sign in to your BYU Account:

1. Go to my.byu.edu
2. Click *Sign In*
3. Enter your username and password and click *Submit*

If you can sign in:

1. Expand the Miscellaneous drop-down in the *Campus Links* section
2. Select the *Change Password/Security Qs* option
3. Reset Password
4. Add/Update Security Questions

If you are unable to sign-in, but have security questions:

1. Make sure you are back at the Sign In page
2. Click on the *Password* link in "Forgot your *NetID* or *Password*"
3. Enter your NetID
4. Answer those questions
5. If entered correctly, a temporary password will be emailed to your email account on file
6. You will use this temporary password at www.byu.edu/password to create a new password

If you cannot sign into your BYU Account or would like help checking the status of your personal information, please call the *BYU Operations and Support Center (OSC)* at *801-422-4000.*

After changing your password, please take the time to perform the following checks and confirm that your data has not been changed:

1. If you are a current BYU employee and you have a premium email account, verify that you can access your email by logging in.
2. Check the inbox rules to see if there are any suspicious rules.
    a. In Outlook, click "Files", "Manage Rules & Alerts", delete any unwanted rules.
    b. For other providers, search online. For example: "Gmail Rules".

3. Confirm your direct deposit information and other financial information is accurate in My Financial Center.
4. Check that your personal information is accurate.
5. Check other information (i.e. parking registration, e-mail alias manager, etc.).

If you have used the same login id and password for other sites and apps, we recommend that you change your password for these as well to ensure you are protected. Ideally, you would have different passwords for each account. For more information on how to secure your online presence, visit besafe.byu.edu.

Our security team is actively working to ensure that victims of these compromises are notified and that their accounts are secured. If you have further questions, please contact the BYU Operations and Support Center (OSC) via call or text (801-422-4000), email (it@byu.edu), or chat (it.byu.edu).

Example request from OCG regarding security incidents

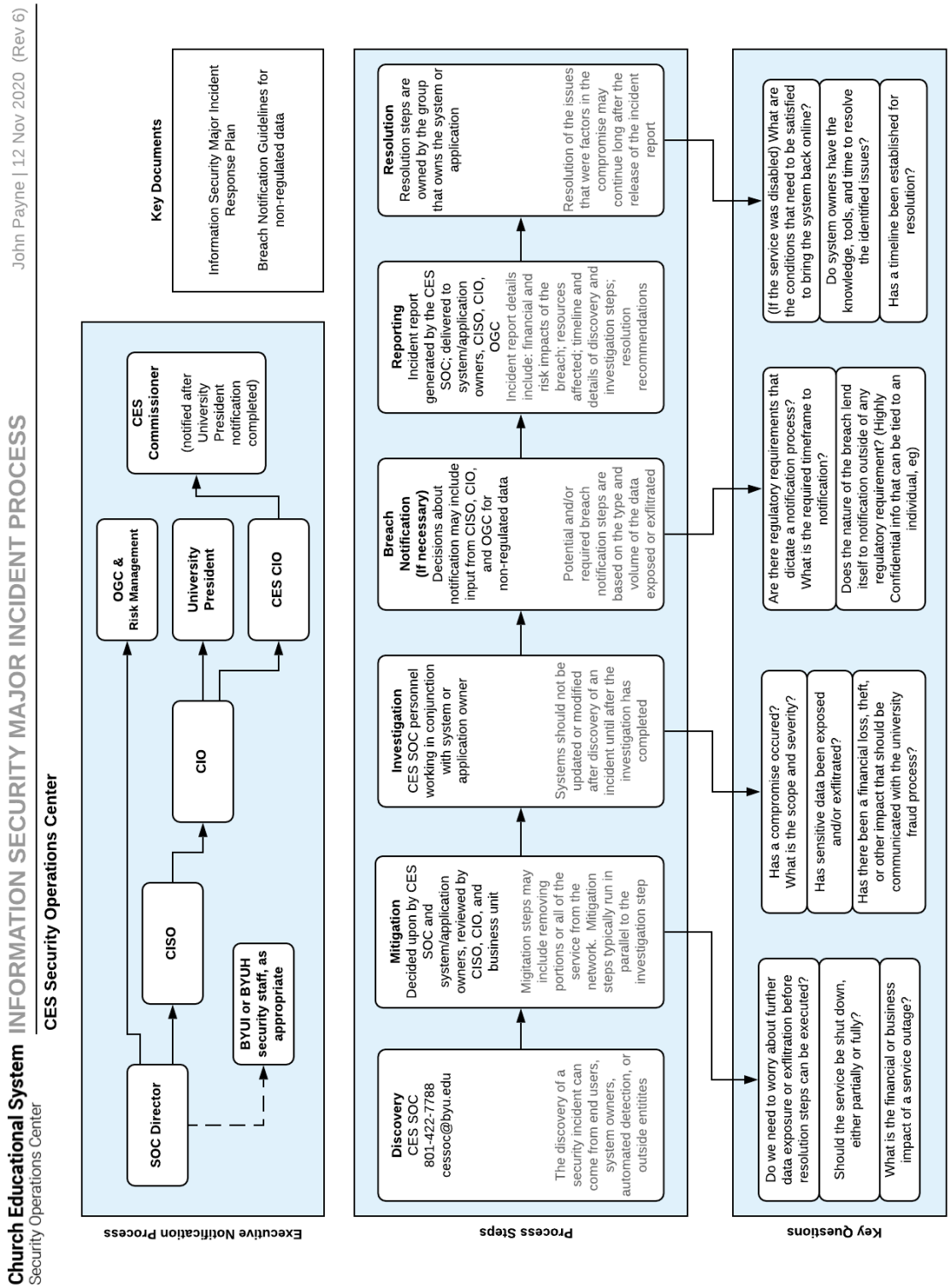
ATTORNEY-CLIENT COMMUNICATION
PRIVILEGED AND CONFIDENTIAL

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



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