



# RESPONSE AND INCIDENT MANAGEMENT PLAN AND PROCEDURES

IT Operations

IT Department  
Epigenome Technologies Inc.



## Table of Contents

<b>Document Revision History</b> .....	2
<b>Data Breach</b> .....	3
<b>Purpose</b> .....	3
<b>Scope</b> .....	3
<b>Participants</b> .....	4
<b>Definitions</b> .....	10
<b>Goal</b> .....	10
<b>Policies</b> .....	10
<b>Procedures</b> .....	10
<b>Information and Intelligence Sharing and Reporting</b> .....	10
<b>Roles &amp; Responsibilities</b> .....	10
<b>Incident Management Flowchart</b> .....	9
<b>Major Incident Management Flowchart</b> .....	10
<b>References</b> .....	11
Appendix A Revised Code of Washington.....	12
Appendix B HIPAA Breach Notification Rule .....	14
Appendix C Process Flowchart for Cybersecurity Event Response.....	16
Appendix D Process Flowchart for Cybersecurity Incident Response.....	17
Security and Privacy Statement.....	18
<b>Incident Request History</b> .....	18



---

## Document Revision History

Description	Date	Author(s)
Ver. 1.0	05/01/2022	Hun Ki Lim & Pei Lin



## Data Breach

A data breach is any instance in which there is an unauthorized release or access of personal information or other information not suitable for public release. This definition applies regardless of whether data is stored and managed directly or through a contractor, such as a cloud service provider. Data breaches can take many forms including

- Hackers gaining access to data through a malicious attack.
- Lost, stolen, or temporary misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.);
- Employee negligence; and
- Risk of, or actual, loss to reputation
- Policy and/or system failure.

## Purpose

This document defines the standards and requires actions for incident management by IT Operations (IT Ops). Additionally, this document outlines IT Ops response procedures in the event of a major incident. This is a dynamic process and will be reviewed and modified as necessary.

## Scope

The scope of this plan and procedures document is to describe Epigenome Technologies Inc.'s response in the event of a security breach of personal information. The plan and procedures will comply with the following laws and standards:


- Revised Code of Washington 19.255.010 : Public Records Act: Personal information -- Notice of security breaches (see Appendix A)
- HIPAA Breach Notification Rule (see Appendix B)
- PCI Data Security Standards

The incident response includes security breaches of computerized systems and/or electronic artifacts (tapes, CD-ROMs) by any individuals including employees, volunteers, contractors, and third-party agency employees.

The incident response includes the activities of assessment, containment, investigation, and notification.

This document should be referenced by IT Security Policy – 01.17.04 so that Epigenome Technologies Inc.'s notification procedures are legally valid, per RCW 19.255.010(8).

The scope of this document does not include breaches of personal information contained in non-computerized (paper) documents. If necessary, a separate policy, and incident response plan and procedures, should be created for unauthorized acquisition of personal information within paper documents.



---

The scope of the first final version of this document will not include the following:

- plan and procedures for responding to security breaches of systems containing confidential data other than personal information
- procedures to automate the monitoring and identification of security breaches
- descriptions of IT security systems, such as firewalls and authentication systems, used to help protect Epigenome Technologies Inc. systems from unauthorized access.

## Participants

Employees in the following positions and departments should be participants in the table-top exercise, and would participate in the event of an actual incident response:

- IT Service Desk
- IT Manager
- Data stewards
- CEO
- Local Law Enforcement
- Budget & Finance Internal Auditor
- Prosecuting Attorney – Civil Division
- Federal Reporting Agencies (NCICC, MS-ISAC)

## Definitions

*After-hours Incident:* Any incident that is discovered or reported outside of normal business hours.

*Call:* a report to the IT Service Desk by a person regarding their observations about an incident.

*Data Steward:* “the department managers or their delegates within Epigenome Technologies Inc. who bear responsibility of the acquisition, development, and maintenance of databases which house Epigenome Technologies Inc. information” (from IT Security Policy – 01.17.04).

*Incident:* an event or series of related security breach events that are being handled by one coordinated response.

*Major Incident:* The primary distinction between an incident and a “major” incident is the number of users affected. A major incident is any event which is not part of the standard operation of a service which causes, or may cause, an interruption to, or reduction in the quality of that service; **and** impacts five (5) or more users.

*Personal Information:* an individual’s first name or first initial and last name, in combination with any of the following data:

- Social security number
- 

- Driver's license number or state identification card number
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Medical or health information collected by Epigenome Technologies Inc. acting as a health care provider, health care clearinghouse, or health plan

*Security Breach*: unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of information maintained by Epigenome Technologies Inc. Examples of security breaches include:

- an employee obtains unauthorized access to a computer system containing confidential information
- a workstation or laptop containing confidential information is lost or stolen
- a hacker breaks into an application server that has access to a database with confidential information
- a department does not properly dispose of a server containing confidential information
- a third-party service provider has experienced any of the above, affecting confidential data related to a Epigenome Technologies Inc. service

## **Goal**

The primary goal of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

## **Policies**

[additions to IT Security Policy - inventory of all reported systems and processes; identify and document all authorized users who access and use personal information; identification of potential security breach notifications]

## **Procedures**

1. An Epigenome Technologies Inc. employee who notices a potential security breach notifies through the Slack channel #IT-Service-Desk at [epigenometechnologies.slack.com](https://epigenometechnologies.slack.com).

2. If the security breach is ongoing and either confidential data or business continuity is at risk the incident will be classified as a “major incident”. The IT Service Desk will collect the following information:
  - Date and time of event
  - Detail description of the event
  - Identification of all hosts (database servers, application servers, etc.) that may be involved.
3. The IT Service Desk notifies the following about the security breach:
  - IT Manager
  - Data stewards
  - Executive
  - Third-party service providers
4. The IT Manager and the director of the data steward’s department may notify the following:
  - Communications (if the security breach is already publicly known, or public notice should be given)
  - Human Resources (if an employee is suspected)
  - Sheriff (if the breach appears to be part of criminal activity)
  - State and Federal Partners as intelligence (NCCIC, MS-ISAC)
  - Local partners (information-sharing)
5. If appropriate, the IT Manager will escalate the incident response to Emergency Management.
6. The primary goal of all responders will be to maintain or restore business continuity, contain the security breach, and to preserve as much evidence in its original form as possible. Each responder will document their actions in Incident\_journal\_entries in internal Dropbox.
7. If, in consultation with the San Diego Prosecutor’s Office Civil Attorney, notification of the security breach is required under RCW 19.255.010, the Communications Director and the Prosecutor’s Office Chief Civil Attorney will approve the wording of the notice and it will be sent to the affected individuals by email, where an email address is available for the individual. A written notice will be sent to affected individuals where an email address is not available for the individual, but a mailing address is available. If Epigenome Technologies Inc. does not have an email or mailing address for some affected individuals, then the notice will be placed conspicuously on Epigenome Technologies Inc.’s public web site.
8. If, in consultation with the San Diego Prosecutor’s Office Civil Attorney and the data custodian, notification of the security breach is required under the HIPAA Notification Rule, the Communications Director and the Prosecutor’s Office Chief Civil Attorney will approve the wording of the notice and notify affected individuals per HIPAA requirements.
9. In the event cardholder data is breached the data custodian is responsible for contacting credit payment system vendor such as Visa, MasterCard, American Express, and Discover within 24 hours of the event and following the specific requirements of the credit payment system vendor. (It is not the general practice of Epigenome Technologies Inc. to store account number or credit

or debit card number numbers in combination with any required security code, access code, or password that would permit access to an individual's financial account.)

## Information and Intelligence Sharing and Reporting

[information sharing vs reporting; when are you *required* to share, when *can* you share, when you *should* share information, and to whom; to possibly include local partners, etc.]

## Roles & Responsibilities

### Incident Management Roles and Responsibilities

Role Name	Role Responsibilities
Incident Manager  <b>NIMS/ICS:</b> Incident Commander (IC)	<p>The Incident Manager role is responsible for the effective implementation of the Incident Management process and carries out the corresponding reporting.</p> <p>This role represents the first stage all cybersecurity events and incidents. This role also declares all necessary escalations.</p> <p>Responsibility for Incident Manager include:</p> <ul style="list-style-type: none"> <li>• Determine command and control locations</li> <li>• Set up Command structure</li> <li>• Coordinate and declare Communications and Respond team managers</li> <li>• Establish priorities</li> <li>• Report to I/T Director, Executive, etc.</li> <li>• Hold periodic status meetings</li> <li>• Contact and coordinate IT Leadership and EOC</li> <li>• Develop after action report and lessons learned</li> </ul>
Communications Manager  <b>NIMS/ICS:</b> Public Information Officer (PIO)	<p>The Communications Manager, or PIO, role is responsible for coordinating communications and updating status information during an incident.</p> <p>Escalation tasks for Major Incidents may include:</p> <ul style="list-style-type: none"> <li>• Obtain a briefing from Incident Manager</li> <li>• Report to Incident Command</li> <li>• Establish call center, and communication protocols and methods</li> <li>• Distribute incident status information</li> <li>• Coordinate communications</li> </ul>



Role Name	Role Responsibilities
Incident Response and Recovery Manager	The Incident Response Manager role is responsible for coordinating the technical response, investigation and recovery for the service(s) affected. This role also owns problem management for root cause determination and resolution.
<b>NIMS/ICS:</b> Operations	Escalation tasks for Major Incidents may include: <ul style="list-style-type: none"><li>• Obtain briefing from Incident Commander</li><li>• Report to Incident Command</li><li>• Develop cybersecurity assessments from a department, system and connection level.</li><li>• Staff core Investigation and Recovery teams</li><li>• Maintain high level incident status list</li><li>• Discover problem(s)</li><li>• Resolve problem(s)</li></ul>

### First-Level - Service Desk

The Service Desk is responsible for the monitoring of the resolution process of all recorded Incidents. Upon discovery or report of an incident, the responsibilities and main actions to be carried out by the (First-Level) Service Desk are:

1. Identify the severity of the incident
2. If the incident is not “Major”, after resolving the incident and document the incident.

### First-Level - Service Desk – “Major”

When a major incident is identified, the responsibilities and main actions to be carried out by the (First-level) Service Desk are:

1. Collect the detailed information about the incident
2. Notify to IT manager

### First-Level – Service Desk – “After Hours”

The Service desk will receive notification of an After-Hours Incident via email or voicemail from the responding support person. The actions to be taken by the (first-level) Service Desk are:

1. Call staff in order listed below.
  - a. Call all staff on list in order. **Do not leave voicemail on first call if no answer.**
  - b. Call all staff on list in order a second time & leave a voicemail for each if no answer.

Hun Ki Lim	619-573-7006
Christopher Hartl	858-260-1119

2. IT Leadership:
  - a. **IF** no contact can be established with the emergency support staff:
    - i. one of the IT managers or Director must be notified:

Name	Position	Home	Mobile
Hun Ki Lim	IT manager		619-573-7006
Christopher Hartl	Bioinformatics Director		858-260-1119

- b. **IF** unable to reach personally, leave a message for each manager & Director.
      - i. After leaving a message for IT Management continue to call IT staff from call list until a live person is reached. – **leaving a message is not acceptable.**

- 
- ii. Upon contact with and IT Cybersecurity staff member, please inform them that “*IT Management has instructed me to inform you that you are now responsible for overseeing resolution of this incident and enlisting others to help solve the problem.*”

### **Specialist Support Groups**

Incidents that cannot be resolved immediately by the Service Desk are assigned to specialists within Second- and Third-Level Support groups.

Specialist support groups will be involved in tasks such as:

#### **Second-Level Support**

All support personnel that are employed by or work within Epigenome Technologies Inc. are considered Second-Level Support Providers; this means that they are part of the internal workforce.

Responsibilities and Standards for (second-level) Support Team handling of incidents.

#### **Second-Level Support – Major**

Slack will be used as a live system. Incident/service data will be entered real time. Updates to assignments and status of incident/service will be kept in the Slack.

Any high priority or major incident with multiple callers will use the following real-time update standards:

Slack and Zoom will be used interchangeably

#### **Second-Level Support - “After Hours”**

Upon discovery or report of an incident occurring outside of normal business hours Second-Level Support will:

Slack and Zoom will be used interchangeably

#### **Third-Level Support**

All support personnel that are external to Epigenome Technologies Inc. are considered Third-Level Support (**Suppliers**); this means that they work for an external company, supplier or vendor. When an incident requires Third-Level resources from external support to assist with investigation of the error, the Second-Level support group assigned to the incident is responsible for engaging the help of those extra resources.

#### **Incident Request History**

The history of an Incident shows the entire life-cycle of the request, it is therefore one of the most important aspects of an Incident to keep up to date. Without a request history ongoing process improvement will not be possible. The journal is one way to show the activity, history and the entire effort needed to resolve the incident. The solution of the incident should be documented in the solution field upon resolution of the incident.

## References

About the PCI Data Security Standard (PCI DSS)

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

## Appendix A

### Revised Code of Washington 19.255.010

#### Public Records Act: Personal information — Notice of security breaches.

(1)(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) For purposes of this section, "agency" means the same as in RCW [42.56.010](#). *[From RCW 42:56.010(1): "Agency" includes all state agencies and all local agencies. "State agency" includes every state office, department, division, bureau, board, commission, or other state agency. "Local agency" includes every county, city, town, municipal corporation, quasi-municipal corporation, or special purpose district, or any office, department, division, bureau, board, commission, or agency thereof, or other local public agency.]*

(2) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

(5) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(a) Social security number;

(b) Driver's license number or Washington identification card number; or

(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(6) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(7) For purposes of this section and except under subsection (8) of this section, notice may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or

(c) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) E-mail notice when the agency has an e-mail address for the subject persons;

(ii) Conspicuous posting of the notice on the agency's web site page, if the agency maintains one; and

(iii) Notification to major statewide media.

(8) An agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(9) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

(10)(a) Any customer injured by a violation of this section may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this section may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

(d) An agency shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.

[2007 c 197 § 9; 2005 c 368 § 1. Formerly RCW [42.17.31922](#).]



---

## Appendix B

### **HIPAA Breach Notification Rule**

Interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the [Federal Trade Commission \(FTC\)](#), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.

#### Breach Notification Final Rule Update

The Interim Final Rule for Breach Notification for Unsecured Protected Health Information, issued pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act, was published in the Federal Register on August 24, 2009, and became effective on September 23, 2009. During the 60-day public comment period on the Interim Final Rule, HHS received approximately 120 comments.

HHS reviewed the public comment on the interim rule and developed a final rule, which was submitted to the Office of Management and Budget (OMB) for Executive Order 12866 regulatory review on May 14, 2010. At this time, however, HHS is withdrawing the breach notification final rule from OMB review to allow for further consideration, given the Department's experience to date in administering the regulations. This is a complex issue and the Administration is committed to ensuring that individuals' health information is secured to the extent possible to avoid unauthorized uses and disclosures, and that individuals are appropriately notified when incidents do occur. We intend to publish a final rule in the Federal Register in the coming months.

Until such time as a new final rule is issued, the Interim Final Rule that became effective on September 23, 2009, remains in effect.

### **Breach Notification Requirements**

Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

- Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact



information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

- Media Notice


Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

- Notification by a Business Associate

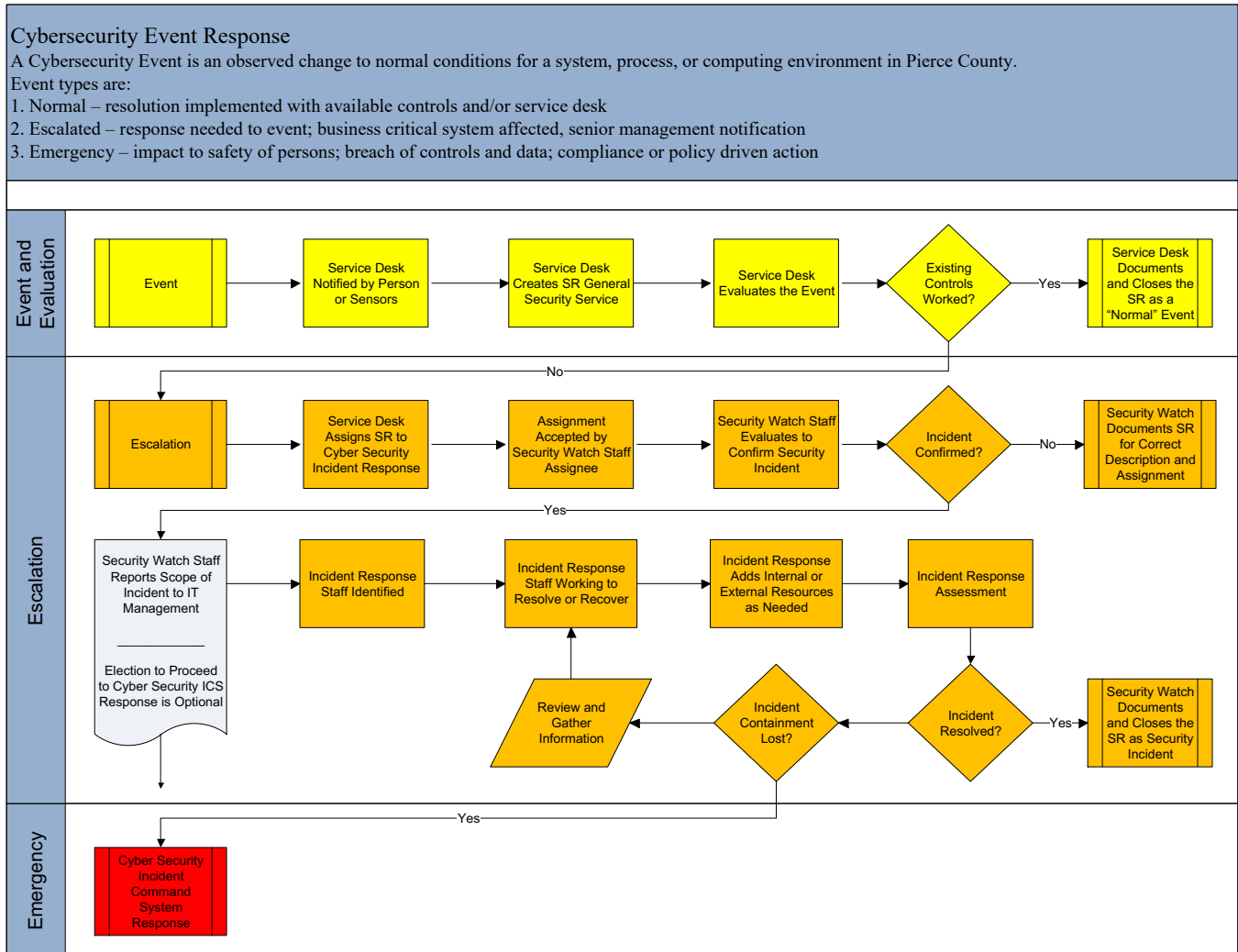
If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.



## Appendix C

### Process Flowchart for Cybersecurity Event Response

#### *EVENT HANDLING*

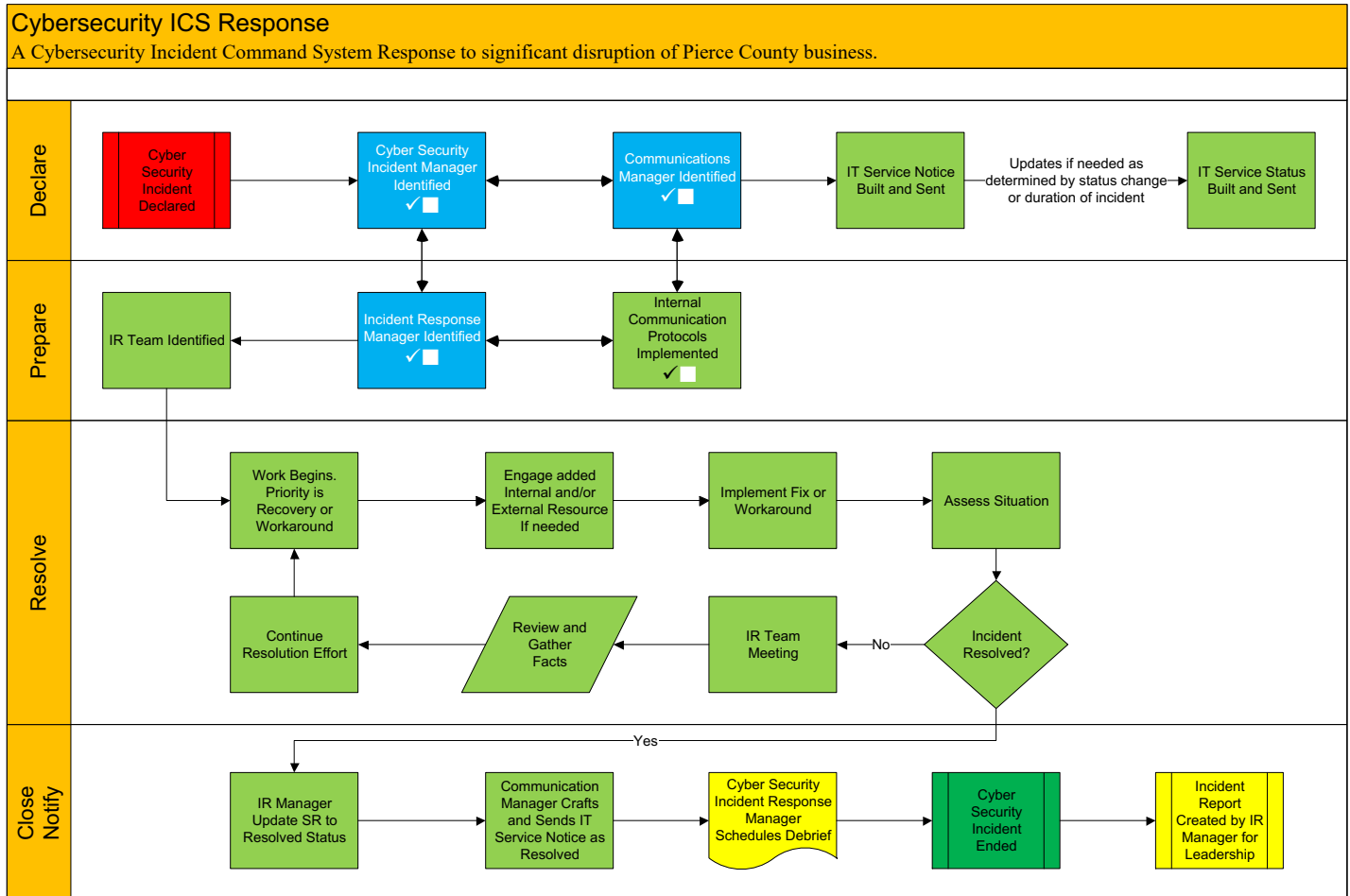


## Appendix D

### Process Flowchart for Cybersecurity Incident Response

#### *INCIDENT HANDLING*

*Cybersecurity Incident response flowchart. This process is established as a means to coordination a response once a declaration of a cybersecurity Incident is made.*



## Security and Privacy Statement

This document is **For Official Use Only**. Portions of this Plan contain information that raises personal privacy or other concerns, and those portions may be exempt from mandatory disclosure under the Freedom of Information Act (see 5 United States Code §552, 41 Code of Federal Regulations Part 105-60). It is not to be released to the public or other personnel who do not have a valid “need to know” without prior approval of the IT Director.

The disclosure of information in this plan could endanger the privacy of employees and could compromise the security of essential equipment, services, and systems of the Information Technology Department or otherwise impair its ability to carry out essential functions.

An electronic copy will be available on the IT intranet and all IT staff will be notified of the plan’s location. Copies of the plan, in a redacted form, may be distributed to other organizations as necessary to promote information sharing and facilitate a coordinated interagency continuity effort. Further distribution of the plan, in hardcopy or electronic form, is not allowed without approval from the IT Director. Updated versions of the plan will be posted on the website as necessary.

### Record of Changes

Change Number	Location of Change	Date of Change	Individual Making Change	Description of Change
Ver. 1.0		05/01/2022	Hun Ki Lim	Initial version

### Record of Distribution

Date of Delivery	Number of Copies Delivered	Method of Delivery	Name of Distributor
5/15/2022	4	Email	Hun Ki Lim