Incident Reporting and Response Procedure: A procedure that provides clear steps to report and respond to a potential cybersecurity incident, from initial detection to containment, eradication, recovery, and post-incident review.

Goals for Cyber Incident Response:

When a cyber security incident occurs, timely and thorough action to manage the impact of the incident is critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals are:

1. Preserve and protect the confidentiality of constituent and employee information and ensure the integrity and availability of systems, networks and related data.
2. Help TKH's personnel recover their business processes after a computer or network security incident or other type of data breach.
3. Provide a consistent response strategy to system and network threats that put TKH's data and systems at risk.
4. Develop and activate a communications plan including initial reporting of the incident as well as ongoing communications, as necessary.
5. Address cyber related legal issues.
6. Coordinate efforts with external Computer Incident Response Teams and law enforcement.
7. Minimize TKH 's reputational risk.

Purpose and Scope

This publication provides practical guidelines on responding to cyber security and data breach incidents in a consistent and effective manner. The plan establishes a team of first responders to an incident with defined roles, responsibilities, and means of communication.

While this plan is primarily oriented around cyber-related incidents and breaches, it can also be utilized for data breaches that are not related to computer systems.

Incident Response Team (IRT)

A team of company staff, advisors, and service providers shall be responsible for coordinating incident responses and known as the Incident Response Team (IRT). The IRT shall consist of the individuals listed in Appendix A, having the noted roles and responsibilities. This team will have both primary members and secondary members. The primary members of the IRT will act as first responders or informed members to an incident that warrant IRT involvement, according to the incident's severity. The entire IRT would be informed and involved in the most severe incidents.

IRT members may take on additional roles during an incident, as needed. Contact information, including a primary and secondary email address, plus office and mobile telephone numbers shall be maintained and circulated to the team. The IRT will draw upon additional staff, consultants or other resources, (often referred to as Subject Matter Experts – SME's) as needed, for the analysis, remediation, and recovery processes of an incident. The Information Technology (IT) function plays a significant role in the technical details that may be involved in incident detection and response and can be considered an SME in that regard.

There shall be a member of the IRT designated as the Incident Response Manager (IRM), who will take on organizational and coordination roles of the IRT during an incident where the IRT is activated for response to the incident.

Incident Response Life Cycle Process

Cyber incident response management is an on-going process with a cyclical pattern. The specific incident response process elements that comprise the Cyber Incident Response Plan include:

1. Preparation: The on-going process of maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, applications, and data handling processes are sufficiently secure, and employee awareness training is in place. Practice exercises (aka Table-top Exercises) for the IRT are conducted periodically, where various incident scenarios are presented to the Team in a practice session.

2. Identification: The process of confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.
3. Notification: Alerting IRT members to the occurrence of an incident and communicating throughout the incident.
4. Containment: Minimizing financial and/or reputational loss, theft of information, or service disruption. Initial communication with constituents and news media, as required.
5. Eradication: Eliminating the threat.
6. Recovery: Restoring computing services to a normal state of operation and the resumption of business activities quickly and securely. Provide reputational repair measures and news media updates, if needed. Provide credit monitoring services to affected constituents, or other remediation measures, as appropriate.
7. Post-incident Activities: Assessing the overall response effectiveness and identifying opportunities for improvement through, 'lessons learned' or mitigation of exploited weaknesses. Incorporation of incident's learnings into the cyber fortification efforts and the response plan, as appropriate.

Incident Occurrence & Awareness

The way an incident becomes known will have an impact on the response process and its urgency. Examples by which becomes aware of an incident include, but are not limited to the following:

1. TKH discovers through its internal monitoring that a cyber incident or data breach has occurred.
2. TKH is notified by one of its technology providers of an incident or becomes aware of the same.
3. TKH is made aware of a breach through a constituent or a third-party informant.
4. TKH and the public are made aware of the incident through the news media.

Incident Response Process Detail

The response process, at a detail level, for an incident includes 5 of the 6 life cycle phases, as it excludes the Preparation phase. The detailed steps and general timing of

an incident response are outlined below. The IT function is specifically called out as an involved party, separate from other SME's.

Process Phase & Approximate Timing	Process Detail Steps	Involved Parties
Identification (Hours)	**1. Identify and confirm that the suspected or reported incident has happened and whether malicious activity is still underway. 2. Determine the type, impact, and severity of the incident 3. Take basic and prudent containment steps.**	**IT and any monitoring service provider**
Notification (Hours – 1 Day)	**4. Inform or activate the IRT, based on the severity of the incident and provide the type, impact, and details of the incident to the extent that they are known. 5. Determine the need for Subject Matter Experts (SME) to be involved in the Containment, Eradication, and Recovery processes.**	**IT & IRT**
Containment (Hours-2 Days)	**6. Take immediate steps to curtail any on-going malicious activity or prevent repetition of past malicious activity. 7. Redirect public facing websites, if needed. Provide initial public relations and legal responses as required.**	**IRT, IT, SME's**
Eradication (Days -Weeks)	**8. Provide full technical resolution of threat and related malicious activity. 9. Address public relations, notification, and legal issues**	**IT, IRT, SME's**
Recovery (Weeks -Months)	**10. Recover any business process disruptions and re-gain normal operations. 11. Address longer term public relations or legal issues, if required, and apply any constituent remedies.**	**SME's, IRT**

Post-incident (Months)	**12. Formalize documentation of incidents and summarize learnings.** **13. Apply learnings to future preparedness.**	**IRT**

Communication Methods

Company communication resources (email, phone system, etc.) may be compromised during a severe incident. Primary and alternate methods of communication using external infrastructure will be established and noted on the IRT member contact list to provide specific methods of communication during an incident. The IRT and any other individuals involved in an incident resolution will be directed as to which communication method will be used during the incident

Information Recording

Information recording is very important during an incident, not only for effective containment and eradication efforts, but also for post-incident lessons learned, as well as any legal action that may ensue against the perpetrators. Each member of the IRT shall be responsible for recording information and chronological references about their actions and findings during an incident.

Incident Response Exercises

The IRT should conduct ‘table-top’ exercises to practice the response process on a periodic basis, but at least annually, so all members of the IRT are familiar with the activities that would occur during an actual incident and their related responsibilities. The exercises may provide the opportunity for enhancing the coordination and communication among team members