PropEx
Cybersecurity Incident Response Plan

Section I. Introduction and Scope

Introduction

PropEx is committed for preventing and protecting the security and integrity of the organization's intellectual property, information assets and resources related to information technology. PropEx understands and recognizes the importance of being vigilant and quick in response to the threat landscape changing often. The following Incident Response plan has mainly been created to direct all the stakeholders and employees to handle the incidents that might have adverse impact on the organization's information resources or assets. The main role of this plan is to help with classifying the incidents to determine the appropriate level of response and remediation based on investigation. This incident response plan is applicable to any individual or entity identified, compelled by any kind of contract or legal enforcements with response to any information security incidents in the organization.

Any individual in the organization suspecting any kind of anomalies or an exposure of PropEx systems, information or any sort of services offered must immediately submit a ticket to PropEx Information Security team at the email address infosecurity@propex.com

Scope

This incident response plan is applicable to any individual or device who has access to PropEx data or systems, to every information systems, PropEx networks and resources. The Cybersecurity Incident Response team that is identified in the plan acts on behalf of the organization in executing the plan and will require and expect the cooperation of all the senior leadership, stakeholders and employees in investigation of the events and incidents as per the requirements.

Maintenance

The Incident Response Team with cooperation of the Incident Handling team will be responsible for maintaining and updating the revision of this document based on annual assessments and findings.

Plan Testing and Review

This Incident Response Plan consisting of various attributes must be tested and reviewed every year. The Chief Information Security Officer will be responsible to conduct and maintain a scheduled awareness and training based on the incidents and events to test response and procedures. Tabletop exercise must be conducted, evaluated responses and identified gaps must be updated in this plan, PropEx policies and procedures as deemed necessary.

Section II. Contact Information

Name	Title	Contact Information
Teja Juluru	Chief Information Officer	tj1057@rit.edu
Pranav Sarma	Chief Information Security Officer	ps4454@rit.edu
Vamsiram Gandham	Cybersecurity Engineer	vg9377@rit.edu
Rohan Mode	Cybersecurity Engineer	rm5532@rit.edu

Section III. Roles and Responsibilities

Cyber Security Incident Handling Team (IHT)

Mainly consists of Risk Managers, Operation Managers, Directors and legal experts that will be notified and consulted in the event.

IHT Role	PropEx Title
Senior Leadership	Chief Information Officer
IHT and CSIRT	Chief Technology Officer
Incident Response Manager	Lead Security Manager
Legal and Communications	Director of Legal Affairs

Cybersecurity Incident Response Team (CSIRT)

The CSIRT mainly comprises Information Technology management and experienced personnel in various areas of business. The main role of the CSIRT is to handle the incidents and events by containment, investigation and recovery of the infrastructure as quickly as possible.

Section IV. Incident Response Framework

The Incident Response framework is mainly adopted to basically identify, protect, respond, and remediate a security incident affecting the company's infrastructure. The framework mainly consists of six phases as follows:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Phase I - Preparation

This phase mainly includes the preparatory measures that our organization must take to safeguard from any potential breach in future. The CSIRT and IHT team are responsible to implement security controls to improve the security posture of the organization.
Phase I is a continuous process and is independent of all other phases.

Phase II - Identification

This phase mainly consists of implementing assessment for the entire organization resources to find gaps in security controls for the same. Mainly the scope, category and potential impact of the alerts generated in the assessment are determined. Further, leads to the detection phase where controls need to be in place for the monitoring and logging purposes.

Phase III - Containment

The main objective of the containment phase is to regain the control of the situation and limit the extent of harm to the infrastructure. To achieve this PropEx has multiple strategies in place which will help to reduce the effect of any incident.

Phase IV - Eradication

This phase mainly consists of eradication of the full elimination of all the components of the incident that happened. Multiple tasks are carried out in this phase based on the incident.

Phase V - Recovery

Once the CSIRT team confirms the eradication of the incident was successfully implemented then all the systems need to be restored back to normal operation. PropEx would always try to implement the installation in a test environment to determine the functionality prior to re-introduction into a production environment.

Phase VI - Lessons Learned

This phase mainly consists of post-incident analysis of all the systems that were targeted and any other vulnerable systems. The objective of this phase is eventually to improve the applicable security operations, response capabilities, and procedures.

Section V - Notification, Communication, and Legal

Required notification and communication both internally with third parties based on regulatory and contractual requirements.

Public Media Handling

All Information concerning an Incident is confidential, and at no time should it be discussed with anyone outside of the Company without the approval of the Chief Information Officer, Incident Response Manager, and/or Director of Legal Affairs. Inquiries from media agencies must be directed pursuant to the Chief Information Officer, Incident Response Manager, and Director of Legal Affairs. Associates found to be discussing an Incident outside of the Company or releasing information about an Incident to a third party without approval pursuant to this section will be subject to disciplinary action, up to and including termination.