PRISM JOHNSON LIMITED

CIN: L26942TG1992PLC014033

Registered Office: 305, Laxmi Niwas Apartments, Ameerpet, Hyderabad – 500 016.
Corporate Office: "Rahejas", Main Avenue, V. P. Road, Santacruz (West), Mumbai – 400 054.

Dated: January 9, 2023

CYBER SECURITY POLICY

Purpose

The purpose of this document is to enable the IT security operations centre team, incident handlers and responders with sufficient information and guidelines to follow when a cyber-security crisis / incident occurs at Prism Johnson Limited (PJL). This document aims at providing detailed information on the steps and the workflow to be followed in the event a cyber-security crisis incident occurs.

Scope

The document applies to all the information technology assets, equipment and devices that are part of Prism Johnson Limited's cyber space environment such as desktops, laptops, applications, servers, databases, network devices, security devices equipment's etc.

The Cyber Crisis Management Plan (CCMP) shall be followed and executed by the employees and vendors deployed by PJL in the IT department providing services to various departments in PJL.

Invocation of Cyber Crisis Management Plan (CCMP)

The major steps followed during invocation of CCMP are as below:

1. I**dentification**
   a. Identification of the incident from all possible channels involved
   b. Verification of the incident if it is a normal incident or a cyber-crisis
   c. Decision of invoking the CCMP shall be taken at this stage

2. **Response and Containment**
   a. Depending on the type of incident, take appropriate action
   b. Inform the affected parties

3. **Communication**
   a. Detailed inputs shall be taken along with other major incident
   b. Timely and continuous communication to all the interested parties viz. at the identification of incident, during the course of incident for action being taken.

4. **Recovery and Preventive maintenance**
   a. Based on the incident resolved, preventive steps to be planned and executed
   b. The recovery and preventive measures shall be discussed and communicated to all the relevant entities in PJL to avoid the happening in near future.

Incident Monitoring and Detection

Primary objective of incident response actions during first hour is to contain the damage due to the incident, notify appropriate authorities about the incident and ensure continuity of essential activities and services.
Analyze the incident based on the data available, define the severity level based on the impact. Take all logs of affected systems for analysis and to correct, eradiate and recover.

Severity Level	Description	Impact	Security Incident Examples
P1	Security breach has occurred and validated. Disclosure of information, user validated Security incident of any Tier 0 system	Highly Notable Outages – complete business interruption due to a breach of information security	Malicious attack or active hacking penetration, in progress for applications. Loss of customer or employee confidential information. Loss of PJL's intellectual property.
P2	Impaired operations due to a security incident resulting in significant business impact.	Impairment of the company's ability to use non-core applications with significant business impact affecting on individual areas with in enterprise	Slow performance of websites due to active web attack. Network bandwidth choke
P3	Minor business impact, isolated security incident on a single system. Unauthorised or inappropriate access.	Applications/components in sub network which is down, resulting is system unavailability to a set of employees, business users or customers in a defined area/location	Data classification error impacting multiple users, repeated failed logins attempts indicating a password cracks attempt. Network device down with workaround. Virus detected on a single machine
P4	Minimal or No Business Impact. Security events requiring additional research	Component, minor application, Sub network down or slow/difficult to use for the users	Non critical security events indicating a security may have occurred but needs to be validated. Data error with workaround , VPN issues, WiFI access point failures

P1 – Critical, P2 – High, P3 – Medium, P4 - Low

Incident Response and Communication

Throughout the cyber security crisis management stages, it is essential that appropriate teams/stake holders shall be notified. This involves communicating to IT and business management levels about the impact and progress of the crisis response.

Department heads will ensure to follow the procedures laid down for the crisis communication is followed.

Stages	Responsible	Accountable	Consulted
Identification	IT Security/Infra/ Digital SPOC	IT Security Head	Information Security Team
Response & Containment	IT & Digital Team	IT & Digital Head	Information Security Team
Communication and Notification	IT Security Head/ IT Infra/Digital Team	IT & Digital Head	CFO
Recovery & Preventive Measures	System Owner	IT & Digital Head	Information Security Team

Exceptions

Where there is a justifiable business need that requires actions to be performed which are in conflict to this document, such exceptions shall be reported to the IT Head and CFO and approval shall be obtained. Such approvals shall be valid for a pre-defined period after which it shall be re-evaluated and re-approved.