Information Security Management Policy

Document Details

Title	Information Security management policy
Version	V.1.0
Classification	Internal
Version Release Date	**1st July 2020**
Version Expiry Date	
Description	
Author	Dipti Chhaniara – DGM IT
Reviewer/Custodian	Ravi Razdan – Head IT & HR
Approved By	Ravi Razdan – Head IT & HR
Owner	IT Department

Version History

Version Number	Version Date
V.3.0	
V.2.0	
V.1.1	
V.1.0	1st July 2020

Table of Contents:

1. Introduction

The purpose of this document is to define a security incident and to provide the procedures for notification and reporting both during and after a security incident.

The scope of this process includes all the information security events / incidents that occur within JLL.

All Employees, Consultants, Contractors, Customers and all personnel who access JLL information systems should report any real or suspected security incident to the appropriate authority immediately.

It is the responsibility of the individual who receives a suspected security incident report to follow the procedures outlined in this document.

2. Security Incident Reporting

Despite an organization's best efforts, a security incident may occur. When an incident occurs, the incident response process helps the affected organization respond to the event and resume normal operations as quickly as possible.

Security incidents or security weaknesses may result in concerns relating to:

- Systems Availability;
- Facility functioning;
- Software Security/ functioning;
- Compromise of confidential/ sensitive information.

  Note: *This is not an exhaustive list.*

Through early detection, an incident response process can provide containment, timely resolution, and preventive measures in dealing with the incident

End Users should be educated on the symptoms of a security incident. Some of the symptoms are as follows:

- Sudden increase in the processor utilization;
- Abnormal increases in file sizes;
- Spam mails or mails from unknown individuals;
- Abnormal shutting down of the system;
- Observed physical security lapses

Note: *This is not an exhaustive list*

Security incidents should be reported as follows:

- A user shall report all security incidents to the appropriate authority i.e. IT.
- The security incident details shall be captured by the IT personnel.

On receiving a Security Incident Report, IT support team should instruct the user to:

- Avoid taking any action that may destroy the required evidence, e.g. shutting down the system etc.
- Avoid discussing the incident with others and taking solutions from everyone.

Note: *This is not an exhaustive list*

Support team analyses the problem and fixes it.

From the time of incident reported to closure support team maintains all the documentation (1.1)

IT Head shall review the logs of all the incidents reported. (1.2)

Annexure

Security Incident Report Form

(To be filled by user identifying the incident)

Security Incident Reported by			
Designation		E-mail	
Date Reported		Time Reported	
Contact Phone Number			
Type of Security Incident	☐ Physical	☐ IT	☐ HR
Location of the Security incident			

If you want to report this security incident anonymously tick this box ☐

Security Incident Details			
What occurred?			
Type of Information compromised			
☐ Confidential	☐ Secret	☐ Restricted	☐ Public
How did you identify the security incident			

Security Incident Response Form

(To be filled up by the ISTF who responds to the security incident)

Security Incident Reported by			
Designation		E-mail	
Date Reported		Reported Time	
Contact Phone Number			
Type of Security Incident	☐ Physical	☐ IT	☐ HR
Location of the Security Incident			

Security Incident Received by			
Designation		E-mail	

Date Reported		Reported Time	

Further Security Incident Details
What occurred?
How it occurred?
Why occurred?
Components affected?
Business Impacts
Any vulnerability identified?

Final Assessment

1.	Status of the security incident	☐ Successful ☐ Continuing	☐ Unsuccessful ☐Suspected
2.	System affected		
3.	MAC Address of the system		
4.	IP Address of the system		
5.	Is the affected system connected to network		
6.	Does the affected system have internet access		
7.	Describe the current security measures provided for the affected system		
8.	Description of the security incident:		
9.	Technical Analyst Name		
10.	Security Incident coordinator Name		
11.	Technical Expert name, if involved		

12.	Response date & time	

	Lessons learnt:
To be signed only after closing the security incident ticket	
Signature of Technical Analyst Date & Time	Signature of Security Incident Manager Date & Time