Security Incident Response Plan (IRP) V1.0

Document information

Prepared By:	Jamie Lovesey	**Copy No.:**	1
Title:	IT Manager		
Reviewed by:	Jamie Lovesey & Andrew Bowden	**Authorised by:**	Andrew Bowden
Title:	IT Manager/Managing Director	**Title:**	Managing Director
Signed:		**Signed:**	
Date of Issue:	1	**Review Date:**	2022
Reference No.:	Information Security Policy	**Version No.:**	1
Supersedes:	1		

Amendment No.	Section No.	Page No.	Paragraph No.	Date	Amended By
1	4.1	9	4	13/09/2022	J.Lovesey

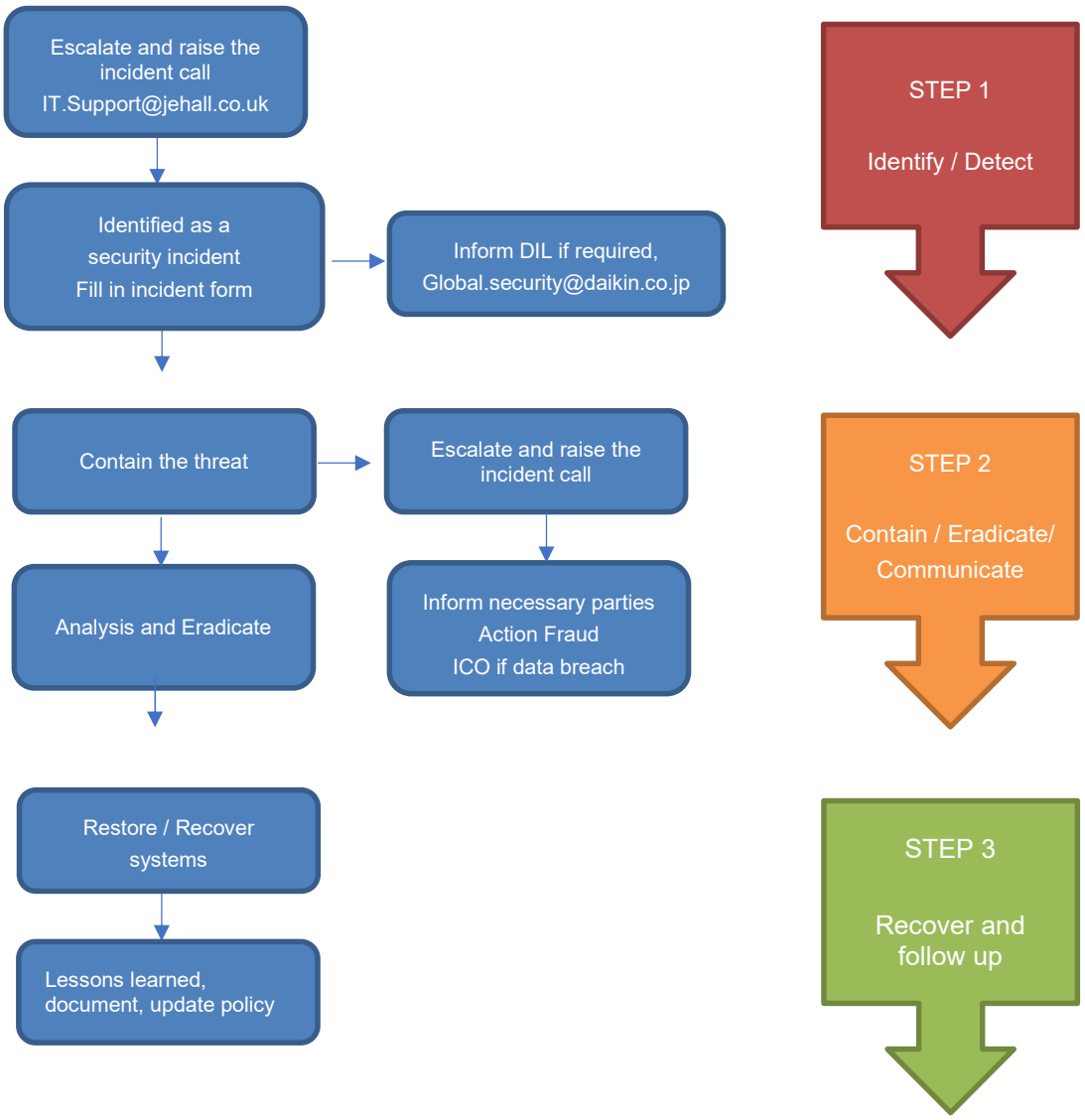
CONTENTS

1. IT Security Incident Response Plan

2. Introduction & Scope

This plan outlines the steps to be followed should Confidentiality, Integrity, or Availability of data being compromised and identifies and describes the roles and responsibilities of the incident response team. This IRP mission is to prevent serious loss of profits, negative public confidence, or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer systems, networks, or databases. The IRT is authorized to take appropriate steps deemed necessary to contain, mitigate, or resolve a computer security incident.

3. Methodology



2.0 Incident identification

An incident by definition is classed as the following ;

"An **Information Security Incident** is an adverse event in an **information** system and/or a **network** that poses a threat to computer or **network security** in respect of availability, integrity and confidentiality"

2.1 Daikin Incident Definition

Information security incident levels are classified into 5: S, A, B, C, and D, and specific response measures are implemented at each incident level. Incident level is determined through discussion by the information security leader and the personnel in charge of response measures applicable for a specific incident level

Level	Definition of level		Examples		
	Impact on the customer and subcontractors	Internal impact	Internal information system	Factory facility system	Product & service system
S	· It can affect human life and who might be affected cannot be identified. · A large amount of personal information can be leaked (*1).	-	· A large amount of personal information such as customer name seems to have been leaked due to malware, etc.	· Hazardous substances can be leaked from the factory due to cyber attacks and can have a serious effect on inhabitation of neighborhood residents.	· Air conditioning facilities in the important infrastructure companies affected by cyber attacks and affect life of unspecified number of people.
A	· It can affect human life and who might be affected can be identified. · A small amount of sensitive personal information (*2) can be leaked.	· It can affect life of employees	· The ID and password for an employee who handles sensitive information such as customer's health condition were leaked and can be abused.	· Malfunction of factory facilities caused by cyber attacks can affect safety for operators.	· Air conditioning facilities in hospital ICU, etc. affected by cyber attacks can cause damages to human life.
B	· Leakage of a small amount of non-sensitive personal information (*1) · Major confidential information leakage · Long-time suspension of services to customers and subcontractors · An event that can affect human body · Possibility of occurrence of any of the above cases	· Major confidential information leakage · Long-term suspension of important operations such as production. · Possibility of occurrence of any of the above cases	· Undisclosed financial closing information, important product design information, etc. seems to have been leaked due to malware, etc.	· Cyber attacks can cause a long-time production line stop.	· Cyber attacks can stop our company's services to be provided to customers all day. · Specific air conditioning facilities malfunction due to cyber attacks and can affect physical conditions of the people around.

Level	Definition of level		Examples		
	Impact on the customer and subcontractors	Internal impact	Internal information system	Factory facility system	Product & service system
C	· It can have a smaller impact on customers and subcontractors than the case described above.	· It can have a smaller internal impact than the case described above	· A PC brought out for external use was lost and part of internal data was leaked.	· The factory facility was infected with malware but it was recovered after the malware was eradicated.	· The product & service system was affected by cyber attacks and customer service response time was temporarily delayed.
D	· No impact occurred on customers and subcontractors, but a security incident occurred.	· No internal impact occurred but a security incident occurred	· A PC was infected with malware, but any problem did not occur.	· The factory facility was infected with malware, but any problem did not was occur.	· The product & service system was affected by cyber attacks, but it did not affect customers.

2.2 JEH classification of incident type

Type of Incident	Description of the incident
Data Breach	Finding confidential / personal information either hard copy oron a portable media device such as a usb pen outside of company premises
Restricted site access	When a person has accessed an area of JE Hall's premises where they are not permitted to, such as entering a server room, or network comms cabinet
Corruption of data	Files on your device or network share are not accessible when other files are, file is opening with non-recognizable characters, or not opening at all and giving errors, or the file has a weird icon instead of the normal expected icon.
Abuse of authorization	An employee has been known to escalate his access rights above what he/she should have, attempting to access network data shares that they should not be accessing
Email malware attempt	An email arrives asking you to click on a link to another website and then enter a username and password
Email social engineering	An email arrives asking you for information and to fill in a website form or reply with what you would class as confidential/ personal information, ask you to provide bank details or payment to the attached pdf invoice but is not from anyone you do business with
Misuse of system	Attempt to login to another person's device, even with their consent. Accessing any part of a database using someone else's password.
Network breach	A non JE Hall employee has managed to attain a username and password from an employee of JE Hall and logs into the system as that member of staff. A 3rd party "non-authorised" device connects onto our core network
Possible of / or a Virus outbreak	Someone clicks on a unknown link and doesn't know if this has triggered a malware / virus. Someone has clicked on the link and now alerts, onscreen messages, or device mis-behaving abnormally.
Loss / Stolen device	Laptop or mobile phone has been stolen, report to police for crime ref number, contact IT dept and line manager. Account will be disabled.
Emailing to wrong recipient	Emailing confidential information to the wrong person or without encryption

2.3 Incident Severity Classification

Critical	All users, All system, All sites.
Major	5+ users, 1+ systems or 1 site is a affected (leakage of data 10,000 files or larger or any personal data as part of GDPR)
Moderate	Less than 5 users, or 1 system
Low	1 user

3.0 Responsibilities

This table identifies the responsibilities. Due to us having limited security tools and applications to inform us of breach it is the responsibility of all JE hall staff that believe there is / was an attempt, or breach to escalate accordingly asap.

The following table defines responsibilities for management and staff J & E Hall Limited.

Director of Finance	The Executive with overall responsibility for Information Security and Data Protection at **J & E Hall Limited**
Senior Manager - HR	Responsible for Personal data: • Liaising with the IT Manager on Information Security Matters; • Managing Data Protection and non-IT related information security on a day-to-day basis; • Reporting on the Data Protection and non-IT related Information Security issues and related activities to J & E Hall Limited Executive Management; • Providing specialist advice, guidance and approvals related to non-IT related of Information Security & Data Protection; • Non-IT related Security Incident & Data Breach Management; • Information Security awareness training; • Providing advice and reviewing third party supplier and service provider contracts and appropriate due diligence in relation to Non-IT related Information Security & Data Protection; • Ensuring all Staff sign and understand the Electronic Communications Policy and receive adequate information and training in respect of the GDPR regulations. • Inform DIL if incident occurs,

IT Manager	Responsible for IT related Information Security including: • Liaising with the Senior Manager - HR on Information Security Policy (this document) and related matters; • Managing IT related Information Security on a day-to-day basis; • Reporting on the IT related Information Security issues and related activities to J & E Hall Limited Executive Management; • Providing specialist advice, guidance and approvals related to use of IT in relation to Information Security; • IT related Security Incident & Breach Management; • Information Security awareness training; • Providing advice and reviewing third party supplier and service provider contracts and appropriate IT related Information Security due diligence; • The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of the IT Department; • Ensuring Security patches are applied promptly and changes are controlled are managed appropriately; • Monitor IT security, revise and adapt the Information Security Policy (this document) to maintain security conditions.
Business Unit Directors	Responsible for Information Security not related to Personal or IT related Information Security. Incidents and breeches must be reported to the Director of Finance.
Directors, Managers, Team Leaders	Responsible for: • Data Protection and Security of Information Assets; • Promoting good Information security practices; • Supporting the IT & Senior Manager - HR in ensuring compliance with Information Security Policy (this document); • Ensuring critical third party suppliers and service providers are appropriately security vetted and an appropriate contract is in place; • Ensuring Data Protection Impact Assessments are completed where appropriate; • Managing Information security risks and solutions; • Notification to customers or suppliers without unnecessary delay where a data breach is likely to adversely affect our customers or suppliers.
System Administrators	Are in a position of trust within the organisation responsible for: • Ensuring they act appropriately and access accounts and systems only in a support situation, where authorised or appropriate; • Reporting any perceived weakness, breach or incident; • Monitoring systems and logs.
All staff	Are responsible for: • Complying with Information Security Policy (this document) and Procedures; • Read, understand and comply with the Electronic Communications Policy; • Protecting internal, confidential and personal data and ensuring it is handled appropriately and secure; • Reporting errors, suspected incidents or issues concerning IT security immediately to the IT Manager; • Reporting errors, suspected incidents, data breaches or issues concerning personal data and non IT security immediately to the Senior Manager - HR; • Staff with permissions for installing software on their own machine are responsible for ensuring it remains patched and supported by the supplier. If the supplier ceases to patch the software, it must be removed.

War Room, Decision making room

Should it be classed as a critical or a major security breach, a war room (decision room) will be created to manage the situation. The key personnel who will participate in the decisions are ;-

- IT Manager
- HR Manager
- Finance Director
- CEO

4.0 Process

4.1 Step 1 – Escalate and Identify

If you believe a security incident has occurred you need to escalate ASAP. The sooner it is escalated and investigated the less threat to the corporate system there is. In the first instance you need to escalate to the IT Security Manager

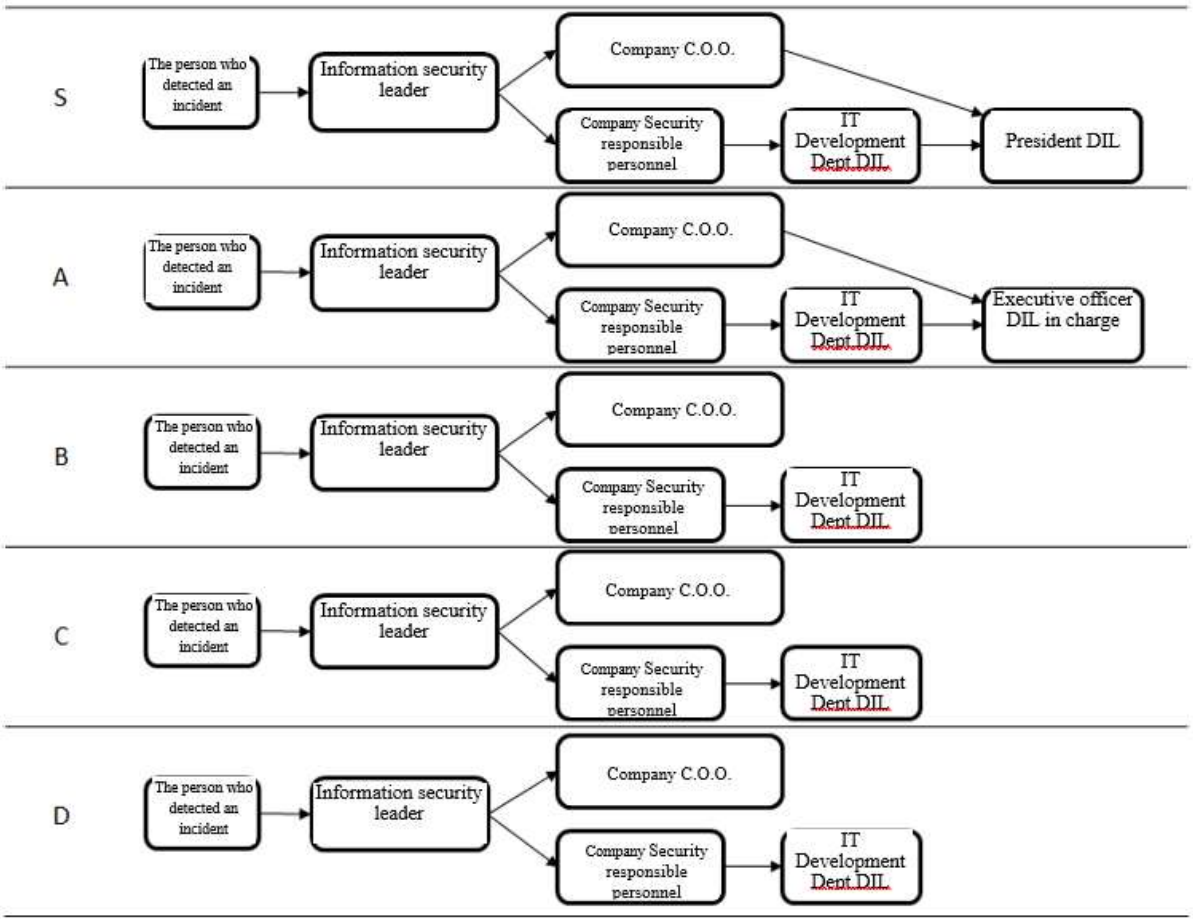
What information you need to provide to the IT Security Manager

Information to provide
• Name who raised the incident, and their contact details • Time that it occurred • Nature of the incident, what occurred • what is the current situation • What equipment, person was involved • Location of equipment or person involved • How the incident was detected • Quantity of staff affected

If it is a member of the IT team who discovers the incident then they will proceed to step 2

The IT Security manager will inform the C.O.O & HR manager and if needed HR will consult with the IT development dept DIL & Global Operations.

Depending on the incident level the following call cascade will be followed ;



4.2 Step 2 Event handling, containing the threat, eradication of the threat

Once the event has been clarified to be a security incident the following actions need to be made.

1. A member of IT will contact you to talk about the incident, and ask for more information to be able to analyze the situation. Depending on the incident all information will be kept classified and staff will be on a need to know basis.
2. IT will then document the situation by filling in a “Security Incident Form”, and start to create a timeline of events, and collate evidence.
3. The IT manager will then inform senior management / stake holders of the situation and provide all the facts about the situation.
4. Depending on the incident severity and type, the effects on the business, users affected, a decision will be made on how to contain the situation, or a war room / critical decisions meeting will take place if the severity is either critical or major. (see Responsibility chart for who will be involved in critical decisions)
5. A broader communication will be sent out to the business to inform staff of the incident and could be asked to undertake necessary actions if required.
6. IT will then eradicate the root cause once identified.

4.3 Step 3 – Restore, system recovery, & lessons learnt

1. Laptops or systems will be restored using recent backups, if these are contaminated the most recent un-contaminated backup will be used.
2. Senior management will be kept informed of progress during the restore, rebuild.
3. If a laptop has been contaminated the device will be reset and restored to previous user settings. If possible, a temporary device will be made available while this occurs.
4. For a period of time the situation will be monitored to ensure the threat has been eradicated
5. A communication of incident closure will be sent out to all staff to brief them on the incident
6. Lessons learned / washup meeting will take place
7. Update plan and or polices to improve future responses.

5.0 Security Incident Form

Reported by		Date reported	
Email		Contact No	
Name of individual concerned		Location of the problem	
Username		Device type	
Description of the problem			

Incident Type

	ELECTRONIC
	Compromised / stolen laptop
	Theft or use of another users ID
	Email spam
	Email phishing attack
	Virus
	Other please explain..

	PHYSICAL
	Unauthorised Access
	Equipment stolen or Damaged
	Data not encrypted on external media
	Confidential documents located outside JE Hall site
	USB pen located with un-encrypted data (no access password)
	Other please explain..

	MISUSE
	Unauthorised use of remote access
	Unauthorised software
	Illegal Log-in attempt
	Storage and use of illegal software
	Inappropriate use of email
	Other please explain..

	MALICOUS CODE ACTIVITY
	Virus scan Engine version
	DAT version
	Date for last scan
	EPO agent installed
	Spam
	Other please explain..