

# **Information Security Incident Management**

Version : 1.0

Proprietary Notice : This document contains proprietary information that is confidential in BPO Convergence company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third part

**Document Revision History:**

Version No	Revision Date	Author	Reviewed By	Approved By
1	15/06/2022	P.Sahoo	S K Patel	P Mohanty
2	10/6/2023	P.Sahoo	S K Patel	P Mohanty
3	13/6/2024	P.Sahoo	S K Patel	P Mohanty

## Contents

1	Policy Statement	1
2	Purpose	1
3	Scope	1
4	Definition	1
5	Risks	2
6	Procedure for Incident Handling	4
7	Policy Compliance	4
8	Policy Governance	5
9	Review and Revision	5
10	References	6
11	Appendix 1 – Examples of Information Security Incidents	7
14	Appendix 2 - Procedure for Incident Handling	9
14	Appendix 3 :Reporting Information Security Events or Weaknesses	11
15	Appendix 4 - Risk Impact Matrix	155

## **1 Policy Statement**

BPO Convergence will ensure that it manages appropriately any actual or suspected incidents relating to information systems and information within the custody of the Company.

## **2 Purpose**

The aim of this policy is to ensure that BPO Convergence manages appropriately any actual or suspected security incidents relating to information systems and data.

## **3 Scope**

This document applies to all Directorates, Departments, Partners, Employees of the Company, contractual third parties and agents of the Company who use BPO Convergence IT facilities and equipment, or have access to, or custody of, customer information or BPO Convergence information.

All users **must** understand and adopt this policy and are responsible for ensuring the safety and security of the Company's systems and the information that they use or manipulate. This includes both data stored electronically and in any other form.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

## **4 Definition**

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

The definition of an "information management security incident" ('Information Security Incident' in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the Company's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

Examples of some of the more common forms of Information Security Incidents have been provided in Appendix 2.

## 5 Risks

BPO Convergence recognises that there are risks associated with users accessing and handling information in order to conduct official Company business.

This policy aims to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up consistently and correctly.
- To help identify and deal with areas for improvement to decrease the risk and impact of future incidents.

Non-compliance with this policy could have a significant effect on the efficient operation of the Company and may result in financial loss and an inability to provide necessary services to our customers.

## **6 Procedure for Incident Handling**

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the BPO Convergence Security Group. The group enables the BPO Convergence Information Communications and Telecommunications (ICT) Department to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the BPO Convergence ICT Department to gain as much information as possible from the business users to identify if an incident has taken place or is occurring.

For full details of the procedure for incident handling please refer to Appendix 3.

## **7 Policy Compliance**

This policy applies to all BPO Convergence employees, Management and any other users of BPO Convergence ICT systems. If any user is found to have breached this policy, they may be subject to BPO Convergence disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

For members this policy will be enforced through BPO Convergence's Code of Conduct for managements.

In such cases the Director in conjunction with the Head of ICT will manage abuse of this policy by undertaking a documented review with the management involved. The review will be recorded and the documents will be retained within the centrally held register.

Two incidents of abuse relating to breaches of this policy within a two year period for the same management could constitute a serious abuse and this trigger point would be reported as outlined below.

Serious misuse of this policy constitutes breach of the BPO Convergence's code of conduct for managements and would be reported to the Group Board of Director, Leader of the Company and the Monitoring Officer. The Monitoring Officer will determine whether the matter should be reported to the Committee.

If you do not understand the implications of this policy or how it may apply to you, seek advice from BPO Convergence ICT Team.

## 8 Policy Governance

The following table identifies who within BPO Convergence is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

<b>Responsible</b>	Head of ICT
<b>Accountable</b>	Center Head
<b>Consulted</b>	BPO Convergence IT Technical Design Authority, BPO Convergence IT Security Group, Officer Governance Group, Human Resources, Union
<b>Informed</b>	All Companylors, Committees, Departments, Partners, Employees of the Company, contractual third parties and agents of the Company

## 9 Review and Revision

This policy, and all related appendices, will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Service Delivery Manager.

### 10 References

This policy should be read in conjunction with all other BPO Convergence policy documents and legal documents including the Electronic Communications Policy



## **Appendix 1 – Examples of Information Security Incidents and Events**

Examples of the most common Information Security Incidents and events are listed below. It should be noted that this list is not exhaustive.

### **Malicious**

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive e-mail to 'all staff' by mistake.
- None reporting of the receipt of unsolicited mail of an offensive nature.
- None reporting of the receipt of unsolicited mail which requires you to enter personal data.
- Changing data that has been done by an unauthorised person.
- Forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others. (Chain letters can be disturbing to those who receive them by implying bad luck if it is not forwarded for example. These are in fact just either at best a piece of fun which clogs up corporate and international email services wasting resource and at worse an attempt to harvest information from the recipients machine including contacts information, details of corporate firewalls etc. They should be deleted straight away and not forwarded anywhere.)
- Unknown people asking for information which could gain them access to Company data (e.g. a password or details of a third party).

### **Misuse**

- Use of unapproved or unlicensed software on BPO Convergence equipment.

- Accessing a computer or database using someone else's authorisation (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

**Theft / Loss**

- Theft / loss of a hard copy file.
- Theft / loss of any BPO Convergence computer equipment.

This policy will be enforced through the use of the BPO Convergence's disciplinary procedures.

Allegations of malicious or misuse will be investigated and action taken in accordance with BPO Convergence's disciplinary procedure. The level of action taken in response to any breach will be dependant on the nature and the findings of any investigation of suspected breaches.

Any suspected breaches of this policy will be managed by the local line manager with assistance from ICT and Human Resources and in accordance with BPO Convergence's disciplinary procedures.

## **Appendix 2 - Procedure for Incident Handling**

### **Reporting Information Security Events or Weaknesses**

The following sections detail how users and IT Customer Services Staff must report information security events or weaknesses. Appendix 1 provides a process flow diagram illustrating the process to be followed when reporting information security events or weaknesses.

#### **Reporting Information Security Events for all Employees**

Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. All users must understand, and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users **must**:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from IT Customer Services Staff).
- Not use any removable media (for example USB memory sticks) that may also have been infected.

All suspected security events should be reported immediately to the ICT Customer Services Team by mail.

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to Senior Management and either the Information Governance Officer (BPO Convergence Pvt Ltd) or Caldecott Guardian for the impact to be assessed.

The ITT Customer Services Team will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and contact number of person reporting the incident.
- The type of data, information or equipment involved.

- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Incident report via email
- Location of data or equipment affected.
- Type and circumstances of the incident.

### **Appendix 3 – Reporting Information Security Events or weakness.**

#### **Reporting Information Security Weaknesses for all Employees**

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Weaknesses reported to application and service providers by employees must also be reported internally to the ICT Customer Services Team. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by the ICT Customer Services Team.

#### **Reporting Information Security Events and Weaknesses for IT Support Staff**

Information security events and weaknesses must be reported to ICT Customer Services who must immediately inform the Business and Customer Services Manager or his representative as quickly as possible and the incident response and escalation procedure must be followed.

Security events can include:

- Uncontrolled system changes.
- Access violations – e.g. password sharing.
- Breaches of physical security.
- Non compliance with policies.
- Systems being hacked or manipulated.

Security weaknesses can include:

- Inadequate firewall or antivirus protection.
- System malfunctions or overloads.

- Malfunctions of software applications.
- Human errors.

Should an appropriate response not be received by the person in ICT Customer Services who owns the logged call within 30 minutes the incident / event must be escalated to the Head of ICT.

Incidents must be reported to the ICT Security Group and the Head of IT&T should the incident become service affecting.

A GovCert Incident report (see appendix 5) must be completed by the incident owner for all incident and passed to the ICT Service Delivery Manager.

### **Management of Information Security Incidents and Improvements**

A consistent approach to dealing with all security events must be maintained across the Company. The events must be analysed and the ICT Security Group must be consulted to establish when security events become escalated to an incident. The incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the Company on continuing operation during the incident.

All high and medium incidents should be reported to the ICT Security Group. All low incidents should be reported to the Customer Services Team Leader. To decide what level of impact an incident has users should refer to the Risk Impact Matrix in Appendix 4.

### **Collection of Evidence**

If an incident may require information to be collected for an investigation strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation, for example concerning computer misuse, contact ICT Customer Services on (55)2222 for advice.

## **Responsibilities and Procedures**

Management responsibilities and appropriate procedures must be established to ensure an effective response against security events. The ICT Security Group must decide when events are classified as an incident and determine the most appropriate response.

An incident management process must be created and include details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
- Limiting or restricting further impact of the incident.
- Tactics for containing the incident.
- Corrective action to repair and prevent reoccurrence.
- Communication across the Company to those affected.

The process must also include a section referring to the collection of any evidence that might be required for analysis as forensic evidence. The specialist procedure for preserving evidence must be carefully followed.

The actions required to recover from the security incident must be under formal control. Only identified and authorised staff should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible.

The officer responsible for an incident / event should risk assess the incident / event based on the Risk Impact Matrix (please refer to Appendix 4). If the impact is deemed to be high or medium this should be reported immediately to ICT Security Group and the Head of IT&T or their representatives.

## **Learning from Information Security Incidents**

To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by the ICT Security Group and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.



### Appendix 4 - Risk Impact Matrix

#### Risk Impact Matrix

To decide on the potential or actual impact of an information security incident, the impact matrix below should be used.

Type of Impact	Reputational Media and Member Damages	Reputational Loss within Government and / or Failure to Meet Statutory / Regulatory Obligations	Contractual Loss	Failure to meet Legal Obligations	Financial Loss / Commercial Confidentiality Loss	Disruption Activities to	Personal Privacy Infringement
Low	None	None	None	None	None	None	None
	Contained internally within the Company Unfavorable Company member response	Internal investigation or disciplinary involving one individual	Minor contractual problems / minimal SLA failures	Civil lawsuit / small fine - less than £10K	Less than £100,000	Minor disruption to service activities that can be recovered	Personal details revealed or compromised within department
Medium	Unfavorable local media interest Unfavorable Company member response	Government authorised investigation by nationally recognised body or disciplinary involving 2 to 9 people	Significant client dissatisfaction. Major SLA failures. Failure to attract new business	Less than £100K Damages and fine	£100,000 - £500,000	Disruption to service that can be recovered with an intermediate level of difficulty. One back up not backing up for 2 or more days	Personal details revealed or compromised internally within authority. Harm mental or physical to one members of staff or public
High	Sustained local media coverage, extending to national media coverage in the short term	Government intervention leading to significant business change. Internal disciplinary involving 10 or more people	Failure to retain contract(s) at the point of renewal	Greater than £100K damages and fine	£500,000 - £1,000,000	Major disruption to service which is very difficult to recover from. Two or more systems not being backed up for two or more days	Severe embarrassment to individual(s)

## Information Security Incident Management

	Sustained unfavourable national media coverage	Service or product outsourced through Government intervention	Client contract(s) cancelled	Over £1M damages and / or fine Custodial sentence(s) imposed	More than £1,000,000	Catastrophic disruption - service activities can no longer be continued	Detrimental effect on personal & professional life OR large scale compromise affecting many people. Harm mental or physical to two or more members of staff or public
--	--	---	------------------------------	---	----------------------	---	---

