Reporting Security Incidents, Breaches, or Unauthorised Access Procedure

Version 1.1

Policy Author	Geoffrey Tanti	**Designation**	Senior Manager IT	**Dept.**	Information Department
Policy Reviewer	Administration Board	**Designation**	N/A	**Dept.**	N/A
Policy Approver	Administration Board	**Effective Date**	15/03/2024		

1. Introduction

1.1 This procedure establishes guidelines for reporting security incidents, breaches, or unauthorised access. The objective is to ensure protection of sensitive information. The purpose of this procedure is to establish a standardized process for reporting security incidents, breaches, or unauthorised access to ensure timely identification, assessment, and response to potential threats to the IfE's information security. Timely reporting is essential to initiate appropriate responses, minimise damage, and enhance overall cybersecurity.

2. Principles

2.1 The IfE fosters a culture of transparency by encouraging employees to report incidents openly and without fear of reprisal.

2.2 The IfE ensures that employees who report incidents are protected from retaliation or adverse consequences as a result of their reporting.

2.3 The IfE holds individuals and departments accountable for their actions and responsibilities related to incident reporting, response, and resolution.

2.4 The IfE maintains accurate and comprehensive records of reported incidents, investigations, actions taken, and outcomes to support accountability, analysis, and reporting.

3. Aims and objectives

3.1 The aims and objectives of this Policy are the following:

- Ensure incidents are reported promptly to enable swift response and resolution.
- Identify and address potential risks and hazards to prevent recurrence and minimize impact.
- Foster a culture of transparency and accountability by encouraging open reporting of incidents.

4. Identification of Security Incidents

4.1 Employees, contractors, or any authorised users who identify or suspect a security incident, breach, or unauthorized access must report it immediately to the IT Department and Data Protection Officer promptly.

4.2 Security incidents include, but are not limited to, data breaches, unauthorised access to systems, malware infections, phishing attempts and any other suspicious activities.

5. Initial Response

5.1 Individuals who identify a security incident should take immediate steps to contain and mitigate the impact, if possible, without compromising the integrity of evidence.

5.2 The individual should immediately disconnect the device from the Internet / Network connection to minimise issues.

5.3 The individual needs to notify the IT department and Data Protection Officer promptly.

6. Reporting Process

6.1 Users are to send an email to the IT support and Data Protection, to report a security incident especially when data breaches are involved.

6.2 Users should provide detailed information about the incident, including the date, time, location, affected systems, and a brief description of the incident.

7. Incident Triage

7.1 Upon receiving a report, the IT department and Data Protection Officer will assess the severity and potential impact of the incident.

7.2 Classify the incident based on predefined categories to determine the appropriate response level.

8. Escalation

8.1 If the incident is deemed severe, the IT department and Data Protection Officer are to escalate the matter to higher management, or any other relevant authorities.

8.2 The IT department and Data Protection Officer are to involve legal, compliance, and public relations teams if necessary.

9. Investigation

9.1 The IT department and Data Protection Officer are to initiate a thorough investigation into the security incident to determine its origin, scope, and potential impact.

9.2 The IT department and Data Protection Officer are to preserve evidence and document findings for analysis and reporting.

10. Mitigation and Recovery

10.1 The IT department is to implement immediate measures to mitigate the impact of the incident and prevent further damage.

10.2 The IT department is to Develop and execute a recovery plan to restore affected systems and services.

11. Documentation and Reporting

11.1 The IT department together with the Data Protection Officer are to document all actions taken during the incident response process.

11.2 The IT department together with the Data Protection Officer are to prepare a comprehensive incident report detailing the nature of the incident, response actions, and recommendations for future prevention.

12. Follow-Up Actions

12.1 The IT department together with the Data Protection Officer are to identify and implement corrective actions to prevent similar incidents in the future.

12.2 The IT department together with the Data Protection Officer are to conduct post-incident reviews to assess the effectiveness of the response and identify areas for improvement.

13. Relevant documents

- Data Protection Act
- Data Protection Policy
- General Data Protection Regulation
- Portal Access Rights Policy and Procedure

14. Version history

Originator	Version	Date	Changes Done
Senior Manager IT	1.0		Initial Release
QA Dept.	1.1	30/04/2024	Updated links