Information Security Management Incident Procedure

1. Introduction

1.1. Employees and sub-contractors using Whitehead-Ross Education and Consulting's (WREC) information systems and services are required to note and report any actual or potential information security incidents occurring in our working practices using the procedure below.

1.2. Information Security incidents can involve:

- Breaches of physical security arrangements
- Unauthorised access
- Human Errors
- Loss, theft or damage of data or equipment on which data is stored
- Misplaced or missing data
- Unclear desk or unsecure screens
- Malfunctions of software or hardware
- Uncontrolled system changes
- Ineffective security controls
- Non-compliance with policies or procedures
- Uncollected printed documents

1.3. Both, potential and actual incidents will vary in impact and risk depending on the content, sensitive nature of the data involved, the circumstances of the loss and the speed of response to the incident.

2. Procedure

2.1. Stage One - Incident response

- Breaches in Information Security must be **immediately** reported to the Managing Director via telephone or, if available, email.
- Inform your line manager
- Depending on the nature of the incident you will be sent electronically, or given a printed copy, of the Information Security Incident Report form from the Managing Director.
- Once completed return the form in the format it was given to the Managing Director along with a copy for your line manager.

2.2. Following the identification and reporting of the Information Security Incident you may be:

- Advised to not continue with that particular work process, in the interim period.
- Asked to assist and provide further information during the investigation.
- The findings will then be reported back to you, by e-mail if applicable, with a copy to your Line Manager.

2.3. Stage Two - Investigation

2.3.1. On receipt of the information, the Managing Director will:

- Input all the information provided onto the Information Security Management Log and allocate a unique number to the incident.
- Further investigate the incident as per the information required from the Breach of Security Data Incident report form.
- Determine corrective action that is to take place, in conjunction with the relevant specialist roles (i.e. Tech Wales).

- Confirm to staff that the affected business systems/processes have been restored and that the required controls are operational before authorising a return to normal working.

2.3.2. Once the incident is contained, and the required corrective action is completed, the Managing Director will report its findings to:

- Management Team.
- Relevant regulators, contract providers (if applicable).
- individual Employee and their line manager (if applicable).

2.3.3. The findings will highlight the cause of the incident and analyse the progress made, whilst trying to identify how Itec could have responded earlier or more effectively, or preventive action that might have been taken in advance of the breach.

2.3.4. The findings will also consider the:

- Effectiveness of the containment.
- Corrective actions.
- Contingency plans.
- External authorities of bodies that should be notified.

2.3.5. In the likelihood of legal, civil or criminal action, the police, lawyers or Independent Authorities must be notified as soon as possible and their guidance for the collection and retention of evidence must be followed.

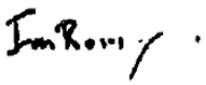
2.3.6. Either the original computer media should be removed and retained securely or copies of information on hard drives, in memory or on removable computer media should be taken (with a log of all actions during the copying process) with a witness present.

2.3.7. On a monthly basis, the Managing Director will distribute a report for the Management Team, which identifies the number, type, category and severity of information security incidents during the preceding month.

2.3.8. If applicable, it will also highlight the cost of containment and recovery of the losses arising from each incident and recommend additional controls that may limit the frequency of security incidents and improve WREC's ability to respond and reduce the cost of response.

2.3.9. Failure to follow this procedure and report information security weaknesses or events can result in disciplinary action against employees, significant company reputational damage and potential fines not including the time and resources involved with rectifying of the weakness or event.

Signed:



Ian Ross
Managing Director

Date: 19th May 2023