Cobseo – The Confederation of Service Charities

Information Security Policy

Policy

The Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of information held by Cobseo – The Confederation of Service Charities. It is the overarching policy for information security and supported by specific other data protection policies.

This policy covers:

Information Security Principles

Governance – Roles and Responsibilities

Security and Security Management

Compliance Requirements

Information Security Principles

The core information security principles are to protect the following information/data asset properties:

Confidentiality – Protect information/data from breaches, unauthorised disclosures, loss of or unauthorised access

Integrity – Retain the integrity of the information/data by not allowing it to be modified

Availability – Maintain the availability of the information/data by protecting it from disruption and denial of service attacks

In addition to these core principles, information security also has important implications on protection of reputation; reputational loss can occur when any of the above principles are breached.

Governance – Roles and Responsibilities

All Staff:

Information Security is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting Confederation business. All staff are responsible for information security and remain accountable for their actions. Staff shall ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

Director of Operations:

The Director of Operations (DoOp) is accountable for information risk within the Confederation and advises the Board on the effectiveness of information risk management across the organisation.

Cobseo – The Confederation of Service Charities

Information Security Policy

All Information Security risks shall be managed in accordance with the Confederation's Risk Management Policy.

Security Management

Technical Security:

Technical security measures detail and explain how information security is to be implemented. These policies cover the security methodologies and approaches for elements such as: network security, patching, protective monitoring, secure configuration and legacy IT hardware & software. This security type is managed, on the Confederation's behalf, by ABF The Soldiers' Charity. For more information on how they protect data, please visit their Information Security Policy.

Operational Security:

The operational security policies detail how the security requirements are to be achieved. These policies explain how security practices are to be achieved for matters such as: data handling, mobile & remote working, disaster recovery and use of social media. Please see Cobseo.org.uk for more.

Compliance Requirements

The Confederation is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Confederation, who may be held personally accountable for any breaches of information security for which they may be held responsible.

Review

This policy shall be reviewed at least annually. The Director of Operations shall be responsible for ensuring the review is conducted in good order and follows due process for approval.

The Director of Operations is accountable for providing the results of ongoing reviews of information security implementation across the Confederation.