INFORMATION SECURITY POLICY

Last reviewed: March 2022

Purpose

The purpose of Integrity Action's Information Security policy is to provide staff with guidelines through which all data that flows through the organisation can be managed responsibly. We aim to align our procedures with best practice; however, given our small size, certain policies are difficult to implement, as we don't have enough people to appropriately break up processes so no one person controls everything. Consequently, it is important that the policies and procedures put in place in this policy are adhered to with great care and discipline.

Ownership and compliance

The responsibility for introduction (including training), consistent application, on-going implementation and periodic review of Integrity Action's Information Security policy lies with the Technology Manager. However, all staff share a responsibility to implement it effectively and to communicate this policy to contractors and consultants connecting to Integrity Action systems.

A staff member found to have violated this policy may be subject to disciplinary action, in line with Integrity Action general disciplinary policy. If found to be in noncompliance, you have the opportunity to challenge the decision.

Compliance Requirements

This Information Security policy adheres with:

1. The Data Protection Act 2018
2. 2CFR200
3. Cyber Essentials (with exception of Router Policy)

List of Integrity Action's Information Security Policy components

The information Security Policy is made of a number of components. Each of the components is being further developed into guidelines, requirements, processes and procedures. You can find a list of these components below.

1. Acceptable Use Policy

This policy serves as an overarching guide that defines what can and cannot be done with Integrity Action devices, including laptops, smartphones, and tablets.

These rules are in place to protect staff members and the organization. Inappropriate use exposes the business to risks including virus attacks, information loss and legal issues.

2. Account Set Up, change and termination policy

The purpose of this policy is to define what level of access is required by new members of staff, consultants, contract workers and those changing position.

3. Administrator-level Privilege Policy

The goal of this policy is to ensure that all individuals that possess administrator-level accounts have been clearly documented and the underlying reasons for the requirement to this level of access is justified.

4. Anti-Virus Guidelines

Integrity Action uses Avast's Business Cloud Care platform to ensure the security of its systems. The Anti-Virus guidelines provide clear instructions to regulate the access of the management dashboard and what processes need to be adhered to reduce the threat of malware.

5. Bring Your Own Device policy

This policy establishes guidelines for staff members and contractors working with the organisation's information systems or data on how to use a personally owned electronic device.

Integrity action recognizes the benefits that can be achieved by allowing staff to use their own electronic devices and the necessity to do so for some contractual positions. Such devices include laptops, smartphones and tablets.

6. Clean Desk Policy / Remote Desk/workspace Policy

The purpose of the clean desk policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about Integrity Action employees, Integrity Action intellectual property, partners and vendors is secure in locked areas and out of site. A

Clean Desk policy is not only ISO 27001 compliant, but it is also part of standard basic privacy controls and vital for an organization now working remotely.

7. Data Breach Response Policy

Should a breach occur and one or multiple Integrity Action Systems become compromised, the Data Breach Response Policy (and procedures) establishes the guidelines for the creation of a response process, allowing Integrity Action to define:

- To whom the policy applies
- Under what circumstances the policy applies
- Staff roles and responsibilities
- Prioritization matrix
- Reporting
- Remediation
- Feedback mechanisms

8. Database Credentials Policy

The Database Credentials Policy provides a set of standards for securely storing and retrieving database credentials, including usernames and passwords in DevCheck:

- Live Environment
- Staging Environment

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Integrity Action or Cloud Enterprises Servers.

9. Disaster Recovery Plan Policy

In the event of a loss of control, disruption or destruction of Integrity Action's information systems, the disaster recovery plan policy serves as the roadmap to recover IT Systems, Applications and Data. This policy establishes the guidelines for the creation of this process. The established process can be found here.

10. Email Policy

The Email Policy assists Integrity Action staff members to know what digital information sent or received should be preserved, over what time period and how this information should be saved.

11. Employee Internet Use Monitoring and Filtering Policy

Compliance standards that Integrity Action has committed itself to require the implementation of monitoring systems which restrict access to malicious websites and record certain activities. The Internet Use Monitoring and Filtering Policy aims to ensure that Integrity Action staff members can use the organisations equipment and systems in a responsible and secure manner.

12. Mobile Employee Endpoint Responsibility Policy

This policy describes what requirements Integrity Action necessitates of its staff and contract workers in relation to the use of mobile devices connecting to organisational resources.

13. Password Construction Guidelines

The purpose of these guidelines is to provide best practices for the creation of strong passwords.

14. Password Protection Policy

The purpose of the Password Protection Policy is to establish a standard for securing passwords.

15. Patching and Updating Policy

The purpose of this policy is to ensure that laptops and other devices used by Integrity Action's staff are kept up to date to prevent the exploitation of vulnerabilities caused by outdated software.

16. Remote Router Policy

The purpose of this policy is to ensure that the router and therefore Internet connection of all remote workers or individuals working on a contract or casual basis for integrity action is adequately secured.

17. Removable Media Policy

Using removable media such as USBs creates a significant risk that Integrity Action data and information may be misplaced or stolen. In addition, the insertion of removable media increases the chance of Integrity Action devices and systems becoming infected with Malware. The Removable Media Policy defines under what circumstances removable media can be used and what steps should be used to mitigate risks.

18. Risk Assessment Policy

Further assessments of organizational information security vulnerabilities must periodically be carried out to ensure continued protection to internal and external threats. The Risk Assessment

Policy establishes what authority and limitation the Technology Manager or other member of staff responsible for carrying out the risk assessment has.

The Risk Assessment Policy subsequently defines what is included as part of the risk assessment.

19. Social Engineering Awareness Policy

The Social Engineering Awareness Policy establishes how information relating to social engineering threats is communicated and how to respond to social engineering threats.

20. Software/Application Installation Policy

The purpose of the Software Installation Policy is to provide clear guidance on what software can be installed on Integrity Action devices, including laptops, smartphones and tablets.

21. Technology Equipment Disposal Policy

Technological equipment used by Integrity Action should be disposed of in a manner that minimizes the impact on the environment and ensures data and any personally identifiable information is scrubbed. This policy provides guidelines on safe disposal of Technology Equipment.

22. Virtual Private Network Policy

The Virtual Private Network Policy provides guidelines for what circumstances require the use of a Virtual Private Network (VPN).

23. Web Application Security Policy

The Web Application Security Policy provides guidelines on how the technology Manager carries out an assessment of web applications (Gmail, Google Apps, etc) in order to identify if systems currently being used adhere to Integrity Action's information standards and to ensure that the confidentiality, integrity and accessibility of the organisation's data and information is not compromised.

This policy lays out what steps must be taken upon the discovery of potential threats and what mitigation strategies are required to reduce attack surfaces and vectors.

24. Minimum Access Policy

This policy makes sure that staff and contractors are aware of the need to minimize access to sensitive information such as personally identifiable information.