Information Security Policy

[April 2022]

Contents

Policy Owner	CIO
Date of last review	March 2022
Date of next review	January 2023
Changes Made:	First Draft for approval at ExCo
Changes Made:	Updated from ExCo
Changes Made:	
Current Version	V1.1

NAME	:	Genevieve Godlonton
SIGNED AS	:	Genevieve Godlonton
SIGNATURE	:	Genevieve Godlonton Genevieve Godlonton (Apr 17, 2023 10:30 GMT+1)
EMAIL	:	ggodlonton@openboxsoftware.com
DATE	:	17/04/23

1. Purpose

The purpose of this policy is to define the objectives and requirements for information security management within Grainger PLC. This policy is supported by a number of other policies referring to specific aspects of information security.

Breaches of this policy may be dealt with under the Disciplinary Procedure which is outlined in the Employee Handbook and, in serious cases, could be treated as gross misconduct leading to summary dismissal.

2. Scope

This policy applies to all Grainger PLC staff irrespective of status, including temporary staff, contractors, consultants and third parties who have access to Grainger PLC's data and systems. The scope of this policy includes, but is not limited to:

- All information processed by Grainger PLC in pursuit of its operational activities, regardless of whether it is processed electronically or in paper form, including but not limited to:
  - External products, materials, information and reports.
  - Operational documents, plans, and minutes.
  - Financial and compliance records.
  - Customer records.
  - Employee records.
- All facilities used in support of Grainger PLC's operational activities to store, process and transmit information (eg offices, build-to-rent sites, areas for remote/home working).
- All external organisations that provide services to Grainger PLC in respect of information processing facilities.

3. Information Security Objectives

The information security objectives of Grainger PLC are the preservation of the **confidentiality**, **integrity** and **availability** of its information:

- **Confidentiality** – This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to the Grainger PLC's information and its systems including its network(s), website(s), and extranet(s).
- **Integrity** – This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency and data back-up plans, and security incident reporting. Grainger PLC must comply with all relevant data-related legislation in those jurisdictions within which it operates.

- **Availability** – This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient, and Grainger PLC must be able to respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

4. Policy Statement

Grainger PLC's information security policy is to ensure that:

- Information security supports Grainger PLC's business objectives.
- Grainger PLC's information security responsibilities are defined and communicated.
- Information security related policies, standards and procedures are in place to identify and mitigate information security risks to an acceptable level, to protect Grainger PLC's systems, infrastructure, and the information security requirements of interested parties, including the organisation's customers and business partners.
- The confidentiality, integrity and availability of Grainger PLC's information and the places where that information is stored, handled and processed are maintained.
- Information security risks to meet Grainger PLC's business objectives are regularly identified and managed
- In the event of a disruption, Grainger PLC can continue to deliver an acceptable level of service for critical activities to its customers.
- Appropriate information security requirements are included in contracts with third parties.
- Grainger PLC's information security related legal and regulatory requirements are met.
- Grainger PLC meets its customer's contractual information security obligations and provides assurance of its capability and capacity to manage information security requirements.

Compliance with this policy is mandatory to minimise business damage by preventing and minimising the impact of information security incidents. Such incidents can result in legal, regulatory or contractual breaches and financial or reputational loss to Grainger PLC and/or its customers.

5. Roles and Responsibilities

- The Executive Committee shall ensure the Grainger PLC continuous security improvement programme is aligned to business objectives, communicate the importance of effective information security management and conforming to policy requirements and provide the programme with sufficient resource to succeed.
- The Chief Information Officer (CIO) is accountable for the continuous security improvement programme at Grainger PLC.

- The IT Director has responsibility for the day-to-day operation of the continuous security improvement programme and for monitoring its performance, reporting to the CIO and Data Protection Committee. The IT Director is supported by a Security & Configuration Manager.
- Legal and Risk are responsible for maintaining an up-to-date list of all legislative, statutory, regulatory and contractual requirements and managing the data protection programme of work at Grainger PLC. They are supported by Data Protection Champions who are located across the business.
- Line managers are responsible for ensuring that their staff comply with this policy. All authorised users shall adhere to this policy. Non-compliance shall be subject to investigation and may result in disciplinary action.

6. Information Security Compliance Management

Activities related to the use of Grainger PLC's information including the systems and places where it is stored and processed shall be monitored to ensure that Grainger PLC's requirements for confidentiality, integrity, and availability are maintained.

Staff or third parties with access to Grainger PLC's information, systems or premises are responsible for reporting any suspicious activity, security breaches or security violations to their line manager, the IT Director or other authorised Grainger PLC contact.

This policy is supported and supplemented by a number of information security related policies, standards and procedures that address specific areas of information security. Several of these documents are referenced as applicable in specific subsections of this policy. The information security related policies, standards and procedures are stored in a central repository and accessible to all relevant audiences.

This policy along with the Acceptable Use Policy are relevant to all staff and third parties who require access

Compliance with applicable information security and data protection regulations shall be enforced, including:

- The European Union General Data Protection Regulation (GDPR) and UK Data Protection Act (DPA) – see the Data Protection Policy.

Any deviation from this policy, or from any of Grainger PLC's information security related policies, standards and procedures, shall only be authorised by the Data Protection Committee if all of the following apply:

- A cost/benefit analysis of the available compliance options and risks of not complying has been performed, and clearly indicates that enforcing compliance would have an unacceptable business impact.
- Risk acceptance has been formally approved and documented.
- Grainger PLC remains compliant with legal and regulatory requirements.

7. Information Security Risk Management

Information security risks shall be identified and managed in line with an established risk management framework. Risks shall be documented in an information security risk register, assessed and prioritised. Appropriate risk treatment options shall be selected and implemented. See the Risk Management Policy for details.

8. Human Resources Security

1.1 Screening

Background verification checks on relevant candidates for employment shall be carried out in accordance with relevant regulations and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. See the Employee Manual for details.

1.1 Awareness and Training

Staff with access to Grainger PLC's information, systems and the places where information is processed shall be educated on their information security responsibilities. Education shall be provided at induction so that new employees understand their responsibilities in respect of the protection of information and places where information is processed and stored.

Staff shall be provided with regular information security education and supporting reference materials as required by applicable regulations. Line managers must ensure the provision of refresher courses and other related materials to regularly remind staff about their obligations with respect to information security.

See the Personnel Security Policy for details.

9. Asset Management

1.2 Information Assets

Assets associated with information and information processing facilities shall be identified and an inventory of such assets will be maintained, with assigned owners. This is covered in detail under the Asset Management Policy.

1.3 Acceptable Use

Rules for the acceptable use of assets associated with information and information processing facilities shall be identified, documented and implemented. See the following policies for details:

- Acceptable Use and Remote Working Policy;

- Mobile Device Policy;

10. Information Security Incidents

Information security incidents can result in legal, regulatory or contractual breaches, service disruption and financial or reputational loss to Grainger PLC and/or its customers. Incidents must be reported via the IT Service Desk application or by telephone (0191 269 5989). Processes and mechanisms shall be in place to:

- Ensure a consistent and effective approach to the management of information security incidents.
- Prevent their occurrence.
- Minimise their impact.

See the following policies for details:

- Incident Management Policy.
- Personal Data Breach Notification Procedure

11. Access Control

Access to information and information processing facilities shall be controlled. Users will only have access to the systems and services that they have been specifically authorised to use. Processes to grant and remove access, and to prevent unauthorised access to systems and applications, shall be applied. This is covered in detail under the Access Control Policy.

12. Physical Security

Security measures shall be applied to:

- Prevent unauthorised physical access, damage and interference to Grainger PLC's information and information processing facilities.
- Prevent loss, damage, theft or compromise of assets and interruption to Grainger PLC's operations.

This is covered in detail under the Physical Security Policy.

13. Operations Security

Processes and mechanisms shall be in place to:

- Ensure correct and secure operations of information processing facilities.
- Ensure that information and information processing facilities are protected against malware.
- Protect Grainger PLC against loss of data.
- Record events and generate evidence.
- Ensure the integrity of operational systems.
- Prevent exploitation of technical vulnerabilities.

This is covered in detail under the following policies:

- Change Management Policy
- Malware Policy
- Backup and Recovery Policy
- Logging and Monitoring Policy
- Vulnerability and Patch Management Policy

14. Communications Security

Processes and mechanisms shall be in place to:

- Ensure the protection of information in networks and its supporting information processing facilities.
- Maintain the security of information transferred within Grainger PLC and with any external entity.

This is covered in detail under the following policies:

- Network Security Policy.
- Encryption Policy.

15. Supplier Relationships

Processes shall be in place to ensure protection of Grainger PLC's information that is accessible by suppliers. Information security requirements, aligned to Grainger PLC's information security related policies, shall be incorporated in contracts with the relevant suppliers. Agreed levels of information security and service delivery shall be maintained, in line with supplier contracts. This is covered in detail under the Supplier Management Policy.

16. Business Continuity

Information security continuity shall be embedded in Grainger PLC's business continuity management system. The availability of information processing facilities shall be insured. This is covered in detail under the Business Continuity Policy.

17. Interested Parties

Grainger PLC has identified the interested parties that are relevant to the continuous security improvement programme and the needs and expectations of those interested parties, listed below. They shall be regularly reviewed and reassessed when changes occur, to ensure that they are understood and appropriately addressed, and that all associated risks, opportunities and issues which may affect the effectiveness of the continuous security improvement programme are identified.

1.4 Roles and Responsibilities

Description	Needs / Expectations
Executive Committee	• Implementation of a continuous security improvement programme supports the Executive Board's vision of successfully delivering and expanding services to Grainger PLC customers.
CIO	• Accountable for the information security strategy and continuous security programme of work with reporting lines to the Executive Committee.
Data Protection Committee	• Support for compliance with Data Protection Legislation • Reviewing the Data Protection at least annually and supporting departmental compliance. • Delivery of the continuous security improvement programme is seen as an enabler to help meet the expectation of all interested parties.

Description	Needs / Expectations
	• Addressing operating environment requirements from regulators. • Expected return in the investment of security related resources – staff, processes and technology.
IT Director and Security and Configuration Manager	• Performance and day-to-day operation. • Identification of enterprise wide IT infrastructure and security requirements. • Identification and deployment of technology to support operations.
Line Managers	• Security framework activities delivering assurance. • Recruiting staff with the necessary level of skills to deliver and support the Information Security Management System. • Deployment of shared technology, with embedded security, to facilitate business opportunities.
IT Department	• Supporting Grainger PLC's business requirements with regards to IT needs, eg networking and computing devices.
Staff	• Expectation that the Information Security Management System will support business requirements across all locations.

18. Policy Review Date

This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection.

Signature: N Papenfus
N Papenfus (Apr 19, 2023 08:44 GMT+2)

Email: npapenfus@openboxsoftware.com

Signature: Sam Duncan
Sam Duncan (Apr 19, 2023 08:46 GMT+2)

Email: sduncan@openboxsoftware.com