NTIA

Information Security Policy

ntia.co.uk

Information Security Policy

Overview

This policy is intended to establish guidelines for effectively creating, maintaining, and protecting passwords at NTIA.

- Introduction

  - Information underpins all of NTIA's activities. It exists in many forms, both electronic and physical, and is stored and transmitted in a variety of ways using company owned systems and those owned privately or by other organisations. Regardless of the form it takes, or means by which it is shared or stored, information should always be protected appropriately.

  - NTIA supports its learners, employees, partners and visitors in allowing them to have access to the information they require in order to carry out their work and recognising the role of information security in enabling this. Information security is characterised here as being concerned with guaranteeing availability (ensuring that authorised users always have access to information when they need it); integrity (safeguarding its authenticity, accuracy and completeness); confidentiality (ensuring that sensitive information is accessible only to those authorised to use it); and disposal (ensuring proper methods of disposal of information that is no longer required).

  - Security of information must therefore be an integral part of NTIA's management and business processes, and a primary consideration for its management structure in order to maintain continuity of its business, legal compliance and adherence to NTIA's own regulations and policies.

  - The Information Security policy underpins NTIA's charter and strategy, and supports NTIA's large and diverse populations who have evolving requirements for information handling and processing.

  - This document provides an overview of Information Security and sets out a series of sub policies that constitute the NTIA Information Security Policy.

- Purpose of the Policy

  - NTIA collects, processes, stores and uses information as part of its academic and business processes. Information may be managed through computerised or manual systems. In all cases, NTIA needs to ensure that adequate controls are in place to ensure information is appropriately available, accurate, secure, and complies with legislative requirements. This Information Security Policy provides management direction and support for information security across NTIA.

  - The Information Security Policy documentation serves these purposes:

- To set out NTIA's intentions in managing information security as part of effective governance

- To provide guidance to users, administrators and developers of information systems on appropriate behaviours and controls required in order to maintain the integrity of information
- To provide a comprehensive approach to information security across NTIA

- Scope of the Policy

  - This Information Security Policy:

    - Applies to all staff, learners, consultants, contractors, partnership organisations and partner staff of NTIA.

    - Covers all information handled, stored, processed or shared by NTIA irrespective of whether that information originates with or is owned by NTIA.

    - Applies to all computer and non-computer-based information systems owned by NTIA or used for NTIA business or connected to NTIA managed networks.

  - This policy should be read in conjunction with the following policies and procedures:
    - Data Protection Policy
    - Cyber Security Policy
    - Malpractice, Maladministration & Whistleblowing Policy

  - This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it to all employees and contracts as applicable.

- Information Security Principles
  - Information will be protected in line with all relevant Legislation and NTIA policies, notably those relating to data protection, human rights and freedom of information.

  - Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset

  - Information will be made available solely to those who have a legitimate need for access.

  - All information will be classified according to an appropriate level of security.

- The integrity of information will be maintained.
- All individuals who have been granted access to information are responsible for handling it appropriately in accordance with its classification.
- Information will be protected against unauthorised access.
- Compliance with the Information Security policy will be enforced.

Governance

- Responsibility for the production, review and communication of the Information Security Policy lies with the General Manager. This policy forms part of the NTIA Company - IT and Data Security Policies Framework.
- The Information Security Policy, including its sub policies will be reviewed annually. Any substantive changes in any of the documents will be communicated to all relevant personnel.

Implementation

- NTIA will:
  - maintain an Information Asset Register (Appendix B)
  - ensure that suitable practices are documented, reinforced and improved
  - ensure that all individuals using information systems and handling information understand the policies and consequences for non-compliance
  - use physical security measures where applicable
  - apply technology where appropriate and feasible
  - use lawful monitoring activities, data and network traffic to detect policy infringements
  - take into account relevant information security requirements when planning and undertaking activities involving information systems
  - undertake risk assessments (Appendix C)
  - monitor the effectiveness of the information security policy

Responsibility

- NTIA is responsible for applying the Information Security Policy to all its Information Assets. This responsibility may be delegated to Heads of Department or Division where appropriate. Individuals must understand and agree to abide by NTIA rules before being authorised to access any information systems for which NTIA has responsibility.

- Compliance, Policy Awareness and Disciplinary Procedures

    - Any security breach of NTIA's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems.

    - The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, and contravenes NTIA's Data Protection Policy.

    - The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against NTIA. Therefore, it is crucial that all users of the NTIA information systems adhere to the Information Security Policy and its supporting policies.

    - All current staff, learners and other authorised users will be informed of the existence of this policy and the availability of supporting policies, procedures and guidelines. Any security breach will be handled in accordance with all relevant company's policies, including the appropriate disciplinary policies.

- Incident Handling

    - If a member of NTIA (staff, learner or partner) is aware of an information security incident then they must report it to the Data Protection Officer via email at mark.masih@jobsinfoods.co.uk
    - Breaches of personal data will be reported to the Information Commissioner's Office.
    - If necessary, members of NTIA can also use NTIA's Malpractice, Maladministration & Whistleblowing policy.

Appendix A

Agreement to Comply Form –
Agreement to Comply With Information Security Policies

Employee Name (printed), **Department**

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to NTIA by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with NTIA, I agree to return all information to which

I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the NTIA security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

Employee Name:

Employee Signature:

Date:

Appendix B

Information Asset Register (IAR) Template

Registered File Archive List							
File No.	Part No.	File Name	Date Closed	File Sent To Archives	Box Details	Destruction Details	Archive Reference Number

Learner Courses Box list		
Learner Company	Course Dates	Learner Details

Registered File Box List	
File No.	File Name

NTIA Registered File List			
Document ID	Document Name	Hard copy Location	Soft Copy Location

Appendix C

Register Assessment Procedure

Reporting, logging and managing information asset risks

Risks that have been assessed should be recorded and reported through line management.

The status of risks should be reviewed regularly by management to decide which of these possible actions is currently appropriate:

Accept	the risk is to be accepted because it's worth taking or is unavoidable
Reduce	measures to help reduce threat likelihood or impact are to be taken
Transfer	responsibility for bearing or mitigating the risk is to be transferred to another individual or organisation
Escalate	it is an unacceptable risk that must be escalated because it cannot be managed locally

Risk ownership should be assigned to an individual or group who realistically can be expected to manage the risk and who could take action deemed necessary for adequate mitigation of the risk.

Risks that cannot be managed by the current risk owner should be escalated.

Proposals for risk mitigation measures are to be considered by management, who will consider factors including whether proposals are affordable and justified.

Where mitigating actions are to be taken, priorities and timescales should also be decided. In addition to a list of threat types, some generic suggestions for mitigation are included in: Information Asset Security Measures (Appendix C).

Senior management should add risks of strategic significance to the departmental risk register for ongoing management and monitoring.

Appendix C (continued)

Risk level matrix:

5	Severe	L	M	H	C	C
4	Major	L	M	M	H	C
3	Moderate	L	L	M	M	H
2	Minor	L	L	L	M	M
1	Insignificant	L	L	L	L	L
Impact		Rare	Unlikely	Possible	Likely	Almost Certain
	Likelihood	1	2	3	4	5

Risk level descriptions detailed on the next page.

Risk level descriptions:

Low (L)	This risk can be tolerated, as the necessary mitigating action is already taken on a routine basis, through established local management processes.
Medium (M)	This risk can still be tolerated, but some additional mitigating action will need to be implemented, beyond that already taken on a routine basis, and monitored by local managers.
High (H)	This risk can only be tolerated if significantly increased and/or additional mitigating action is implemented and closely monitored by senior management.
Critical (C)	This risk cannot be tolerated. A detailed and comprehensive action plan will need to be implemented as a matter of urgency, and closely monitored, with the aim of reducing this risk to a lower level.

Signed:

Date: