Information Governance Information Security Policy

Document Type: Issued

Version No: 2.0
Issue Date: 1st Aug 2020

Purpose of this document

To provide Junkshon with a Corporate Information Security Policy.

VERSION HISTORY

Version	Date Issued	Brief Summary of Change	Owner's Name
V1.0	01/01/2020	Initial Draft	Justin Campbell
V2.0	01/08/2020	Updated with IDS framework	Justin Campbell

For more information on the status of this document, please contact:	legal@Junkshon.com
Date of Issue	01/08/2020

Policy title:	**Junkshon Information Security Policy**

Issue date:	01/08/2020	**Review date:**	01/07/2020

Version:		**Issued by:**	

Aim:	Provide policy guidelines for Information Security matters relating to the operation of Junkshon its services and application and associated information technology components.

1. Introduction

This top-level information security policy is a key component of Junkshon's overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

2. Objectives, Aim and Scope

2.1. Objectives

The objectives of Junkshon Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Junkshon by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

2.3. Scope

This policy applies to all information, information systems, networks, applications, locations and users of Junkshon or supplied under contract to it.

3. Responsibilities for Information Security

3.1. Ultimate responsibility for information security rests with the Chief Executive of Junkshon but on a day-to-day basis the CIO shall be responsible for managing and implementing the policy and related procedures.

3.2. Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

3.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

3.4. The Information Security Policy shall be maintained, reviewed and updated by the CIO This review shall take place annually.

3.5. Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

3.6. Each member of staff shall be responsible for the operational security of the information systems they use.

3.7. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

3.8. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

4. Legislation

4.1. The Junkshon 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 Junkshon who may be held personally accountable for any breaches of information security for which they may be held responsible.

5. Policy Framework

5.1. Management of Security

5.2. The Junkshon Security Officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

5.3. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

5.4. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

5.5. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

5.6. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

5.7. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

5.8. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

5.9. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

5.10. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

5.11. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the CIO and the Information Governance.

5.12. Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of junkson's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.13. Information security events and weaknesses

All information security events, and suspected weaknesses are to be reported to the [insert appropriate officer title and contact details]. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.14. Classification of Sensitive Information.

A consistent system for the classification of information within Junkshon organisations enables common assurances in information partnerships, consistency in handling and retention practice.

Junkshon shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance.

In order to meet Junkshon's organizational and contractual requirements with respect to data handling, the following data classification framework will be used.

Data Classification	Notes
Unclassified	Publicly accessible open data e.g. content published on the Junkshon.com website or readily available to the public. No business impact if data compromise occurs.
Junkshon Confidential	Junkshon internal data related to the business operations and intellectual property of Junkshon. Significant business impact to Junkshon if data compromise occurs. Requires protective measures in terms of data loss prevention, encryption and data access.
Client Confidential	Data shared with Junkshon by clients that the client regards as confidential. Significant business impact to Junkshon and its clients if data compromise occurs. Requires protective measures in terms of data loss prevention, encryption and data access.

Junkshon personnel should ensure that all data is appropriately labelled as to its classification.

All three data classifications are suitable to be deployed on to an accredited public cloud.

5.15. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation’s property without permission from the CIO Users breaching this requirement may be subject to disciplinary action.

5.16. User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of CIO before they may be used on Junkshon systems. Such media must also be fully virus checked before being used on the organisation’s equipment. Users breaching this requirement may be subject to disciplinary action.

5.17. Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

5.18. Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the CIO before they commence operation.

(Organisations are encouraged to develop a series of System Level Security Policies (SLSPs) for systems under their control in order to distinguish between the security management considerations and requirements of each. In this way, specific responsibilities may be assigned, and obligations communicated directly to those who use the system. A separate illustrative template will be provided to aid the local development of these SLSPs).

5.19. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the CIO.

5.20. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the CIO. Users shall not install software on the organisation’s property without permission from the CIO. Users breaching this requirement may be subject to disciplinary action.

5.21. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

5.22. Reporting

The Information Security Officer shall keep the [insert appropriate Board] informed of the information security status of the organisation by means of regular reports and presentations.

5.23. Further Information

Further information and advice on this policy can be obtained from

6. Intrusion Detection Systems

Intrusion detection is a critical piece of junkshon's security policy. Effective security systems must evolve to handle the vast amount of vulnerabilities introduced by the use of distributed systems. Having some type of reassurance that the systems and network are secure is important, and intrusion detection systems can help provide part of that assurance.

The purpose of this policy is to provide guidance for the use of intrusion detection at junkshon. This document is to be followed for intrusion-detection monitoring using intrusion detection tools and system audit logs for the system servers, software, database, networks, and firewalls under its control.

This policy applies to all constituents at junkshon's More specifically, this policy applies to all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resource security.

24/7 intrusion-detection monitoring will be conducted by using intrusion-detection tools and system audit logs for the system servers, software, database, networks, and firewalls under its control.

Alerts are generated and sent to the junkshon messaging system; the alerts are reviewed for possible corrective action.

Procedures for system break-ins:

- Immediately notify management via a predefined emergency notification list and notify the affected network manager.
- Follow up with a system security report to management in the System Security Template, as shown in the following example. The report will include an assessment on compromised systems or information, system risks, and corrective actions.
- Security management will determine the appropriate corrective action and direct the corrective action based on priority.

Other procedures include the following:

- Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- Audit logging of any firewalls and other network perimeter access control system must be enabled.
- Audit logs from the perimeter access control systems must be monitored/reviewed daily by the system administrator.
- System integrity checks of the firewalls and other network perimeter-access control systems must be performed on a routine basis.
- Audit logs for servers and hosts on the internal, protected network must be reviewed on a weekly basis.
- All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
- All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the Incident Management Policy.

CIO
legal@junkshon.com