Robinson Services Ltd

Information Security policy

1.0 POLICY STATEMENT

1.1 Introduction

The security of information in all its forms is fundamental to the operation of Robinson Services. It is recognised that Robinson Services must protect its information assets. All company information, in any form, whether related to internal Robinson Services business, or to that of our customers and clients, must be handled with discretion and should not be discussed or disseminated outside the company without authority. This will enable Robinson Services to fulfil its mission, protect its reputation and ensure that a high-quality service can continue to be offered to our customers and clients.

When it is appropriate to disseminate company information, the “Need to Know” principle shall be applied. This means that if someone does not need to know the information to do his / her job, that person must not be given it.

1.2 Security Objective

Our security objective is to protect Robinson Services from security threats that might adversely impact our operations. This includes threats to Confidentiality (unauthorised access or provision of information), integrity (information being altered without permission, whether deliberate or accidental), and availability (information not being available when it is required). This broad definition of information security also includes authentication (ensuring that access is provided to the right person) and repudiation (incontrovertible provision of information).

1.3 Approach

a) We use the BS ISO/IEC 27002 Code of Practice for Information Security Management as a framework for guiding our approach to managing security of information.
b) We use HM Government standards for information security as required in UK government contracts, and other relevant government’s standards if working outside the UK.
c) We comply with the requirements of the Data Protection Act 1998, the Data Protection (Amendment) Act 2003 and Directive 2002/58/EC of the European Parliament and of the Council about holding and handling personal information.
d) We will comply with relevant Client Security Policies as required in specific contracts.
e) We will use all reasonable, appropriate, practical and effective security measures to achieve our security objectives.
f) We will continually examine ways in which we can improve our use of security measures to protect and enhance our business.
g) As a responsible organisation, we will protect and manage our information assets to enable us to meet our contractual, legislative, privacy and ethical responsibilities.

1.4 Responsibilities

Everyone within Robinson Services is responsible for protecting our information assets, systems and infrastructure. They will, at all times, act in a responsible, professional and security-aware manner, according to the principles laid out in this policy.

Everyone will protect information assets that are entrusted to them, whether such protection is required contractually, legally, ethically or simply out of respect for other individuals or organisations.

All employees are responsible for identifying shortfalls in our existing security practices and/or improvements that could be made. These should be reported to their Operational Director. The Managing Director is responsible and accountable for ensuring that our security objective is achieved.

All management activity shall actively encourage security best practice amongst their employees. Senior Management is responsible for allocating sufficient resources so that Robinson Services realistically can achieve its security objectives. This includes people, time, equipment, software and access to external sources of information and knowledge.

The IT Manager for Robinson Services is the System Security Officer responsible for information held on Robinson Services servers.

Robinson Services Managing Director is responsible for ensuring all standards of security are adhered to within Robinson Services.

1.5 Practices

We use risk assessments as set out in BS ISO/IEC 27002 to identify our security risks and their relative priorities, responding to them promptly and confidently, implementing safeguards that are appropriate, effective, culturally acceptable and practical.

Very sensitive information, the unauthorised disclosure of which could harm the company, our customers and clients requires a security classification identifying it as subject to special handling and storage. Employees must ensure that information is correctly classified and that it is handled and stored securely. If in doubt, ask your line manager.

Sensitive documents, when no longer required, must be destroyed correctly by using a cross-cut shredder.

1.5.1 Documents

CONFIDENTIAL is the only classification to be used for sensitive material in Robinson Services. Its use should be limited to sensitive documents, whether on paper, electronic or other media. The following illustrate what constitutes sensitive:

a) Senior level documents and minutes of meetings
b) Project specific information
c) Financial matters
d) Legal matters
e) Personnel documents and records.

Use of the classification Secret is not to be used unless it appears on Government-related contracts and business.

1.5.2 Need to Know, Need to Hold

The “Need to Know” and “Need to Hold” (i.e. need to retain and store) principles govern the dissemination of documents and a conscious decision regarding these aspects is to be taken by any originator/holder of classified documents. Robinson Services applies an enhanced screening process (“vetting”) to those who are permitted access to classified material to confirm their integrity, reliability and discretion.

1.5.3 Need to Take

Management approval is required before any classified document is taken out of a Robinson Services office, and return is to be confirmed on the next working day by the authorising manager or their nominee. All employees at Robinson Services will be accountable for their actions and all actions will be attributable to an identified individual by effective use of security controls.

1.5.4 Disclosure of Information

Robinson Services information will only be disclosed to third parties when their need to know has been consciously assessed and with clear undertakings on its subsequent use. Information owners are responsible for identifying to whom their information may be released and on what terms. Information will be held and released in line with all relevant legislation, e.g. Data Protection Act 1998; Freedom of Information Act 2000; Official Secrets Act 1989.

Deliberate unauthorised disclosure of information to, for example, the Press, a competitor, or anyone not authorised to receive it will be treated as a serious breach of contract and will result in disciplinary action, up to and including termination of employment.

1.5.5 Projects

Any project for which there is a project specific “insider” list shall be classified as CONFIDENTIAL. The insider list shall specify who is briefed on and party to a sensitive project. The list is to be maintained by a nominated individual engaged on the project (normally the person responsible for the security of the project) and each person on the list is to be provided with a copy of the latest iteration of the list in order that they know with whom they may discuss the project. Each person initiated into a project will sign an undertaking to discuss the project only with those colleagues also listed.

1.5.6 Other Documents

Unless falling into one of the categories outlined above all other Robinson Services documents are to be treated, by default, as for internal use only, unless expressly marked to the contrary.

1.5.7 Addressee Only

In circumstances where there is a reason for limiting the “need to know”, the privacy marking “Addressee Only” shall be annotated to the document. In this case ONLY the addressee should open the envelope. This applies, for example, to project documents.

1.5.8 Additional Privacy Markings

Consideration should be given to extra caveat markings, which further clarify handling, distribution and storage, for example “Retain until…”, “Destroy after …”

1.5.9 Personal

The restrictive marking “Personal” may be used on documents of a personal rather than a business nature. This shall not be used on Robinson Services documents.

1.5.10 Dangers of Over-Protection

Over-protection will not only “clog up” the system and Robinson Services, but ultimately will also bring it into disrepute. Additionally, attempts at over-protection may lead to contractual limitations on disclosure of classified information being declared void in a civil court action.

1.6 Preparation of Classified Documents

1.6.1 Creation

Before creating a sensitive document, consider whether or not it really needs to be set out in writing.

1.6.2 Preparation

All stages of preparation of sensitive documents (note making, telephone calls, dictation, drafting and word processing) shall be carried out under conditions allowing no accidental or deliberate overlooking or eavesdropping by unauthorised persons. Particular care shall be taken to ensure the security of tapes and discs which have been used to record dictation or telephone conversations of a classified nature. Telephones should not normally be used for discussing matters of a classified nature. Waste products (notes, drafts etc.) shall be destroyed as classified waste.

1.6.3 Shared Printers

When printing classified documents to shared or remote printers the author shall ensure that no one else is standing at the printer and shall remove documents from the printer without delay. If the remote or shared printer has a ‘secure print’ password option, this is to be enabled and used at all times when printing classified documents.

1.6.4 Marking of Documents

ALL CONFIDENTIAL documents shall be marked clearly with the classification, preferably at the centre of the top and bottom of every page.

CONFIDENTIAL documents may additionally be given an individual copy number (e.g. copy no.1 of 6 copies) which shall be marked on the top right-hand corner of the front page. The file copy shall show the copy number dispatched to each named addressee. Authorised extra copies shall be marked “repro copy”, e.g. “repro copy 1 of 1” in order to distinguish them as such. The consent of the originator of a CONFIDENTIAL document must be obtained before copies are made and the originator must be given details of the additional addressees in order to retain a master list of distribution.

When a document requires a classification for a limited period only, e.g. figures ahead of publication, the document shall be suitably endorsed “To be declassified on (date/time)”.

1.6.5 Distribution and Dispatch

Classified / sensitive documents shall be sent to internal addressees in a sealed envelope (see Addressee Only above). When such documents are dispatched to outside recipients, they shall be double enveloped (internal envelope marked Addressee only), and sent by Courier or recorded delivery service. Recipients (internal and external) shall be provided with a tear-off receipt on which to confirm receiving their copy. There must be no visible indication on the envelope of the fact that the contents are classified.

It should be exceptional for sensitive / classified documents to be sent by fax (see section below). If there is an unavoidable requirement to send them by e-mail, they must first be encrypted.

A copy of the distribution list for each classified document must be retained for 2 years, together with the receipts.

1.6.6 Reproduction

All classified document reproduction shall be carried out under the direct supervision of a nominated person who will ensure that the correct number of copies is made and that all spoiled or excess copies are retrieved and destroyed under secure conditions. This shall include electronic copies.

1.6.7 Storage

All sensitive / classified documents must be kept in a lockable steel cabinet to which access is controlled. The holder of the key or combination must be a person authorised to see classified material.

1.6.8 Destruction

Cross-cut shredders are essential for secure destruction of classified papers. They cut documents both vertically and horizontally; simple lateral shredders cut documents lengthwise only and the resultant strips can be re-assembled. Authorised recipients must supervise personally the destruction of sensitive data, documents and information media. Confidential waste receptacles may only be used if they are lockable and are emptied and disposed of by a Robinson Services approved supplier.

1.7 Information Technology Systems & Equipment

1.7.1 Networks and Infrastructure

Robinson Services IT infrastructure is protected centrally by a fully managed firewall. We use SonicWALL equipment and our firewall is managed by an IT Provider who monitor and configure the device and security services to detect and protect against potential security threats. All the latest software updates and patches are updated onto our firewall as they become available and the firewall’s advanced security services also act as a first line of defence scanning traffic for viruses, malware and blocking intrusions.

Robinson Services internet access is provided by two BT fibre circuits. We also use a dedicated circuit to connect to our Disaster Recovery data centre. It is important to Robinson Services that access to the many areas where our business rely on internet access, from email, web browsing, supporting remote workers, applications and increasingly software, is completely secure and reliable. Our internet access sits inside our managed network and behind our firewall.

1.7.2 Passwords and Systems Security

Passwords are an important aspect of our computer and systems security and are the front line of protection for all user accounts. Robinson Services treats the use of passwords very seriously and has a published ‘Password Policy’. The policy applies to all Robinson Services employees, contractors and vendors with access to systems operating within Robinson Services. Passwords are issued and managed by departmental senior staff with responsibilities for administering access to individual systems.

Robinson Services also use additional methods of authentication for employees requiring remote access to our internal network and systems.

Robinson Services uses Microsoft Remote Desktop Services within our network. This consists of two main components: a perimeter security solution and a software solution for the users. RDS reduces the risk of infected machines connecting to our network and minimises the number of ports we need to open on our firewall. RDS access is provided via an encrypted VPN connection where the external party has restricted access to the internal network. This prevents devices external to the Robinson Services network from being able to infect the internal network or access resources to which they are not entitled.

1.7.3 Servers

Robinson Services server equipment is housed in a secure Comms Rooms that is climate controlled. Robinson Services has a Disaster Recovery server located off-site at a secure data centre. Both comms room and data centre have access control systems in place.

1.8 Security Policy Review

The Board owns this policy and is committed to the implementation of it. Adherence to the policy will be monitored on a frequent basis to ensure compliance. The policy will be reviewed annually or more frequently if required due to legal, operational or best practice reasons. The policy will be regularly reviewed for completeness, effectiveness and usability. Effectiveness will be measured by Robinson Services ability to avoid security incidents and minimise resulting impacts, together with a process for benchmarking security maturity with other similar companies and establishments.

It is required that year on year there will be an improvement in security maturity within Robinson Services. This improvement will be measured and reported on throughout the year.

The Board will sign off all new versions of the Security Policy. All employees of Robinson Services are responsible for identifying ways in which the Security Policy might be improved. Suggestions for improvement should be addressed to the Managing Director. Unless immediate changes are required, suggestions will be discussed at the annual review of the policy.

1.9 Policy Awareness

The security policy is available to all employees via the 'Robinson Services' intranet and may also be contained in any relevant site/office manuals.

All employees are expected to be familiar with, and to comply with this policy at all times. The Managing Director will be responsible for interpretation and clarification of the Security Policy.

Employees requiring education about any aspects of this policy should discuss their needs with their line manager.

1.10 Applicability and Enforcement

This policy applies to all employees and visitors to Robinson Services. Robinson Services mandates compliance to this policy within employees' terms of employment.

Failure to comply with the Security Policy could harm Robinson Services ability to achieve its mission and/or damage the professional reputation of the establishment or that of a customer or allied organisation. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

The Managing Director will be responsible for all decisions regarding the enforcement of this policy, utilising Robinson Services Human Resources team to execute the disciplinary procedures as appropriate.

1.11 Incident Management

All breaches of information security, actual or suspected, are to be reported to the IT Manager and the relevant Regional Director. All IT incidents will be reported to GovCertUK http://www.govcertuk.gov.uk by the IT Manager.

David Robinson
Group Managing Director
1 March 2018