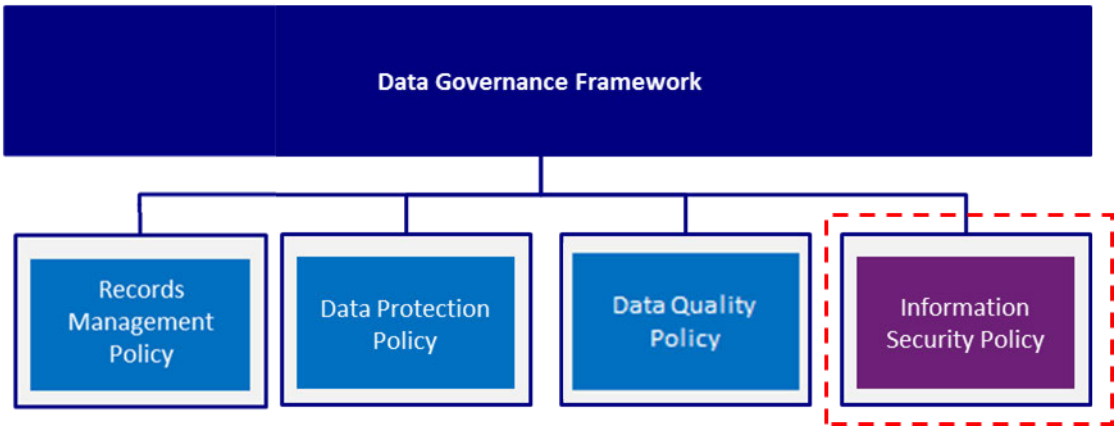
ROAD SAFETY AUTHORITY

ICT Security Policy

This policy sets out to define the security controls necessary to safeguard Information Systems that process RSA information



Document	ICT Security Policy	**Version**	2
Originator	[redacted]	**Issuer**	[redacted]
Page 1 of 12 pages		**Issue Date**	15 December 2017

Document Control

Version History

Version	Date Released	Contributor	Description
1	17 October 2016	[redacted]	ICT Steering Group Approved for publication
2	15 December 2017	[redacted]	Redrafted for approval by senior management team
3	14 February 2019	[redacted]	Published a third party version of the RSA ICT Security policy

Document Approval

Approved By	Position	Date
Management Team		15 December 2017
ICT Management Team	Head of ICT	31 January 2019

RSA ICT Security Policy

Introduction

Information is a critical asset of the Road Safety Authority ('the RSA'). Accurate, timely, relevant, and properly protected information is essential to the success of the RSA's strategy. The RSA is committed to ensuring all accesses to, uses of, and processing of RSA information is performed in a secure manner.

Information Systems include but are not limited to all infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store information owned by the RSA.

The objective of the ICT Security Policy is to define the security controls necessary to safeguard Information Systems that process RSA information and ensure the security, confidentiality, integrity and availability of the information held therein.

All RSA third parties that store, process or transmit RSA information must comply with this policy. The controls outlined in this policy will be used to directly assess third parties to ensure uniform implementation of information security controls throughout all systems that process RSA information.

The Senior Management Team of the RSA have approved the ICT Security Policy.

Legal Requirements

The RSA has an obligation to abide by all relevant Irish and European legislation. The relevant acts, which apply in Irish law to Information Systems, include but are not limited to:

- Data Protection Acts (1988 and 2003)
- Criminal Justice (Theft and Fraud Offences) Act, 2001
- Freedom of Information Act, 2014

Consideration is also made of the following legal instruments that are due to come into effect in May 2018.

- Directive on Security of Network and Information Systems (NIS Directive)
- European General Data Protection Regulation

The RSA also processes credit card information and so must be compliant with the PCI DSS.

Related Policies

This policy should be read in conjunction with the following policies.

- Data Governance Framework
- Data Protection Policy
- Data Quality Policy
- Records Management Policy
- ICT Acceptable Usage Policy

1. User Access Management

User Access

All systems must be designed and implemented with the following considerations made

1.1. Separation of Duties – For Tier 1 solutions (see appendix A) and sensitive functions such as finance transactions, granting licenses, user access management and technical system changes, there must be separation of duties to avoid the possibility of collusion.

1.2. Least Privilege – For Tier 1 solutions, users should only be able to perform the actions (including accessing data) that they need to perform their role.

1.3. Need to Know – Access to all systems should ensure that only information that is required for a role is available to each category of user.

1.4. Single points of failure – Solutions must be designed and supported in such a way that there are no user single points of failure in support or operation of solutions.

1.5. Unique Accounts – All users of systems must use unique accounts and not share passwords with anyone. Administrator account use must be minimised and only used when required.

1.6. A secure password policy must be applied to all network / computer logon and Tier 1 solutions (see Appendix A)

1.7. Systems should integrate with RSA Active Directory where possible

2. System Security Architecture

This section only applies to third parties who are hosting the solution. If the RSA data centre is being used to host the solution, then the RSA ICT infrastructure team will be responsible for meeting below requirements.

2.1. Firewalls must be used to define a perimeter and secure inbound / outbound traffic to non-secure networks (i.e. Internet)

2.2. Firewall rules must be reviewed on an annual basis to check for insecure configuration and overly permissive rules.

2.3. Network Intrusion Detection / Prevention Systems (NIDS) must be used to monitor traffic on any network segments that support the transfer of RSA information.

2.4. An inventory of all IT systems and software installed on networks that support the processing of RSA information must be maintained.

2.5. All system components must provide audit trails of all relevant security activities. Audited activities must include at least the user, action performed and time performed for the following actions

- Any access to personal information, including read, write and search of personal information.
- Any changes to public facing website content
- Any approvals that are made
- All changes to user administration
- Any attempts by users to enter malicious content in to the application

2.6. Security logs must be reviewed on a regular basis for any security incidents.

2.7. Anti-Virus (AV) software must be installed on all desktops and Windows servers. All systems must have virus definitions within at least three days for active systems. All systems must perform full system scans at least weekly for active systems.

2.8. Host Intrusion Detection / Prevention software (HIPS) must be installed on all Servers and Desktops.

3. Tier 1 Solutions

3.1. All Tier 1 solutions (see appendix A for definition) must have a design document containing at least the following

- Network diagram including all IP addresses and ports that need opening on the firewall
- Information flow diagram
- Details of user roles and access control matrix
- Data retention must be defined for all categories of data including any personal data, user access data and general log data
- Details of backup procedures for system configuration
- Details of backup procedures for data
- Details of BCP, DR aspects of the design
- Comprehensive software component inventory
- Incident response plan

3.2. All Tier 1 solutions must have a separate test environment for testing new releases / patches / fixes. Production data must not be present in test environments. Test data should not appear in production.

3.3. File Integrity Monitoring (FIM) software must be installed and configured on all servers that support Tier 1 solutions.

3.4. All Tier 1 solutions must have a backup, BCP and IT DR contingencies in place. These should be tested at least on an annual basis.

3.5. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of the recovery plans must be defined for all Tier 1 solutions.

4. Vulnerability Management

4.1. All software / hardware components must be in support and appropriately licensed.

4.2. All software / hardware components must apply security updates to the Operating System, Database and Application according to the following timescale.

- Critical / High issues – 2 months
- Medium issues – 6 months
- Low issues – 12 months

4.3. All Application, Web Servers, Databases and Operating Systems must be hardened prior to go live with documentation detailing hardening steps (such as those specified in CIS, NIST standards)

4.4. There must not be any default / shared accounts on Operating System, Database or Application.

4.5. All new systems must be subject to a passing vulnerability scan and penetration test before go live.

4.6. All system components must be subject to a quarterly vulnerability scan with issues addressed according to the timescale in 4.2.

4.7. All Tier 1 systems must have a network and application penetration test report in the last 12 months with issues resolved according to the timescale in 4.2.

5. Application Security

5.1. Source code must be securely managed and Intellectual Property retained by the RSA.

5.2. Authentication to applications across insecure networks (i.e. the Internet) must have two factor authentication incorporating two of the following

- Something you have – approved examples include mobile phone (SMS, App)
- Something you know – approved examples include password, security questions
- Something you are – approved control is biometrics

5.3. Applications, especially that are part of Tier 1 solutions, must have been developed in accordance with good practice development standards. This is expected to include

- Developers must have an awareness of common application vulnerabilities such as those in the OWASP Top 10.
- Projects on Tier 1 solutions must undertake a documented threat modelling exercise on the solution.

6. Data Security

6.1. All customer and employee personal data must be protected at rest and in transit using approved cryptographic algorithm and protocols (See Appendix B).

6.2. Private keys / passwords must be kept confidential. All usernames and passwords must be encrypted when in transit. Passwords must be salted and hashed using an appropriate algorithm.

6.3. No customer data sets can be stored on public cloud environments.

6.4. All hard drives that contain or may have contained sensitive information must be securely disposed.

6.5. All portable devices such as laptops, smart phones and tablets that process RSA customer information must be encrypted.

6.6. All third parties that access networks, either through VPN or company assigned equipment must sign the Network Access Rules.

6.7. All third parties that access networks that process and/or store RSA information must be reviewed on an annual basis, either by RSA or someone appointed by RSA, to ensure that they have equivalent security controls as to the ones detailed in this policy.

6.8. For instances where services have been subcontracted it is the responsibility of the contractor to ensure compliance with 7.2.

6.9. All subcontracted third parties that process RSA data must be compliant against this policy, areas of non-compliance must be notified the RSA account manager as soon as possible but not later than one 1 months after discovery.

6.10. The RSA reserve the right to audit 3rd parties against this policy at a mutually agreed date.

6.11. The RSA will carry out penetration testing on all publically available IT services owned by the RSA. Third parties that are responsible for supporting Tier 1 IT services are required to remedy any vulnerabilities discovered during penetration testing in the timelines outlined in section 4.2.

7. Incident Management

7.1. Incident Management processes must be approved by the RSA. For Tier 1 solutions these must include a framework of different severity levels for incidents, roles and responsibilities for employees that may be involved in an incident and escalation of any incidents that

- Cause downtime of more than one hour
- Involve the possible or actual compromise of RSA information

7.2. All IT security incidents must be reported to the RSA account manager.

7.3. Incident reports must be provided after 2 hours (incident notification), 5 days (incident resolution) and 15 days (root cause analysis and action plan) after an incident is discovered. The reports must contain whatever information is available containing at least the following

- Description of the incident response steps taken
- The number of records / systems affected
- The type of data processed by the systems
- The time of discovery of the incident (the time when the incident was discovered)
- The period of time that the incident was active (the time of compromise to the time of remediation)

7.4. For Tier 1 solutions, Incident Response Plans should be tested on an annual basis.

Appendix A – Acronyms and Definitions

Acronym	Definition
ICT	Information and Communications Technology
BCP	Business Continuity Plan – This refers to contingency plans required for critical business processes.
RPO	Recovery Point Objective – The maximum targeted period in which data might be lost from an IT service due to a major incident
RTO	Recovery Time Objective – The duration of time within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.
IT DR	IT Disaster Recovery – This refers to the technical recovery of IT solutions
CIS	Centre for Internet Security – This is a non-profit organisation dedicated to enhancing the cybersecurity readiness and response among public and private sector entities
NIST	National Institute of Standards and Technology - US technology agency that works with industry to develop and apply technology, measurements, and standards.
OWASP	Open Web Application Security Project – This is a non-profit organisation that provide good practice guidance on building and maintaining secure applications
PPS	Personal Public Service Number (PPS number) is a unique reference number that is required to access social welfare benefits, public services and information in Ireland.
AES	Advanced Encryption Standard – Widely regarded a secure encryption algorithm
3DES	Triple DES (Data Encryption Standard) – Insecure encryption algorithm
ECDH	Elliptic Curve Diffie–Hellman Key Exchange – Algorithm used for key establishment
SHA	Secure Hash Algorithm. There are a number of versions that have various levels of security
MD5	Insecure Hash Algorithm. This should be avoided where possible.
TLS	Transport Layer Security – cryptographic protocols that provide communications security over a computer network. There are a number of versions that provide various levels of security.
SSL	SSL (Secure Sockets Layer) is an insecure security technology for establishing an encrypted link between a web server and a browser.
SSH	Secure Shell – Cryptographic protocol used to log on to remotely logon to systems

POP3	Post Office Protocol version 3 is a standard mail protocol used to receive emails from a remote server to a local email client.
IMAP	Internet Message Access Protocol is an standard protocol used by e-mail clients to retrieve e-mail messages from a mail server
SNMP	Simple Network Management Protocol is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on a network.
FTP	File Transfer Protocol is a standard insecure network protocol used to transfer computer files between a client and server on a computer network.
VPN	Virtual Private Network – Protocol that encrypts traffic across insecure networks
PCI DSS	Payment Card Industry Data Security Standards

Term	Definition
Customer personal data	This may include any subset of driver details such as driver name, date of birth, address, telephone number, email, PPS number, credit card details
Employee personal data	This may include any subset of employee name, date of birth, address, telephone number, email, PPS number, banking information, payroll information, grade
Customer personal data set	This refers to the collection of 5 or more instances of customer personal data. There are particular restrictions on the use of customer personal data sets.
Tier 1 Solutions	This refers to an IT solution that contains significant amounts of either customer personal data or employee personal data or that perform sensitive functions such as finance applications. These solutions have more stringent security requirements

Appendix B - Encryption Algorithms and Protocols

Note - Where the algorithm / protocol is not listed it is up to the ICT team to specify compliance status.

Supported symmetric encryption algorithms

- AES 256

Examples of unsupported symmetric encryption algorithms

- 3DES, RC4

Supported asymmetric algorithms used for key establishment

- RSA (2048 bits), ECDH (384 bits)

Example of unsupported asymmetric encryption algorithms

- RSA with less than 2048 bits

Supported hash functions

- SHA-256, SHA-384, SHA-3

Example unsupported hash functions when used to support Tier 1 solutions

- SHA1, SHA2
- MD5

Supported cryptographic protocols

- TLS v1.2, SSH v2 in counter mode

Examples of unsupported cryptographic protocols

- SSL v2, v3, TLS v1, TLS v1.1, SSH v1, SSH v2 with CBC mode

Examples of unsupported protocols

- FTP, telnet, POP3, IMAP, and SNMP v1 and v2