Operating Procedure
Patching

Document Classification:	Public
Document Ref.	ISMS-DOC-A12-1-6
Version:	1.0.3.1
Dated:	29 May 2018
Document Author:	John Moylan
Document Owner:	John Moylan

Revision History

Version	Date	Revision Author	Summary of Changes
1	21/12/2016	John Moylan	Initial Draft
1.0.1	21/12/2016	John Moylan	Minor Edits
1.0.2	8/2/2016	John Moylan	Incorporate feedback into section 1.1.1
1.0.3	28/3/2017	John Moylan	Reclassified 'Public'
1.0.3.1	29/5/2018	John Moylan	Reviewed and version incremented. No other changes

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Contents

1 Operating Procedure

RTÉ is responsible for ensuring the confidentiality, integrity, and availability its data and that of customer data stored on its systems. RTÉ has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

1.1 Scope of Procedure

This policy applies to workstations or servers owned or managed by RTÉ. This includes systems that contain company or customer data owned or managed by RTÉ regardless of location. The following systems have been categorized according to management:

- Unix/Solaris servers and appliances
- Microsoft Windows servers and appliances
- Linux servers and appliances
- Workstations (desktops, Mac's, laptops and MacBooks)

1.1.1 Related Policies

Web Application Security Policy

1.2 Policy

Workstations and servers owned by RTÉ must have up-to-date (as defined by RTÉ's Information Security team minimum baseline standards) operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by RTÉ.

1.2.1 Workstations

Microsoft Desktops and laptops will have updates pushed out to them via Microsoft SSCM each month and will be a maximum of one month in arrears for updates. This is the default configuration for all workstations built by RTÉ. Any operating systems that are no longer covered by upstream support and deemed unsupportable by RTÉ will not be permitted to use RTÉ resources. Any exception to the policy must be documented and forwarded to the Information Security team for review. *See Section 1.4 on Exceptions.*

1.2.2 Servers and appliances

Servers must comply with the minimum baseline requirements that have been approved by the Information Security team. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the RTÉ asset and the data that resides on the system. Any operating systems that are no longer covered by upstream support and deemed unsupportable by RTÉ will not be permitted to use RTÉ resources. Any exception to the policy must be documented and forwarded to the Information Security team for review. *See Section 1.4 on Exceptions.*

1.2.3 Roles and Responsibilities

- **The technical manager** responsible for each area will be responsible for coordinating patching needs for Windows, Linux, Unix and Solaris servers and appliances in their area. And will be responsible for ensuring that systems are patched to a level as defined by RTÉ's Information Security team minimum baseline standards. Any exception to the policy must be documented and forwarded to the Information Security team for review. See Section 1.4 on Exceptions.

- **Technology Infrastructure** will manage the patching needs for the Microsoft Windows servers on the network.

- **Technology Infrastructure** will manage the patching needs of all workstations on the network.

- **Information Security** is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.

- **The Change Management Board** is responsible for approving the monthly and emergency patch management deployment requests.

1.2.4 Monitoring and reporting

Active patching teams noted in the Roles and Responsibility section 1.2.3 are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Information Security and Internal Audit upon request.

1.3 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all employees at RTÉ Information Security and Internal Audit may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the RTÉ issue tracking system and support teams shall be dispatched to remediate the issue. Repeated failures to follow policy may lead to disciplinary action.

1.4 Exceptions

Exceptions to the patch management policy require formal documented approval from the Information Security Team. Any servers or workstations that do not comply with policy must have an approved exception on file with the Information Security Team. *Please refer Information Security Team for details on filing exceptions. All exceptions will be regularly reviewed.*

1.5 Definitions

Term	Definition
Patch	A piece of software designed to fix problems with or update a computer program or its supporting data
Trojan	A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
Worm	A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

1.6 Minimum baseline requirements for servers and appliances

The default baseline for all systems to be a maximum of not more than one month in arrears for upstream patches. From time to time, critical issues may require that this patching deficit be reduced.