

Ref:	NR/L2/INF/02242/01
Issue:	1
Date:	05 March 2016
Compliance date:	07 June 2016

Information Security Manual

Module 01 – Acceptable Use of Information and Information Systems

.....

This document is the property of Network Rail. It shall not be reproduced in whole or part nor disclosed to a third party without the written permission of Network Rail.
© Copyright 2016 Network Rail.

Uncontrolled copy once printed from its electronic source.

Published and Issued by Network Rail, 2nd Floor, One Eversholt Street, London, NW1 2DN.



Ref:	NR/L2/INF/02242/01
Issue:	1
Date:	05 March 2016
Compliance date:	07 June 2016

User information

This Network Rail standard contains colour-coding according to the following Red–Amber–Green classification.

Red requirements – no variations permitted

- Red requirements are to be complied with and achieved at all times.
- Red requirements are presented in a red box.
- Red requirements are monitored for compliance.
- Non-compliances will be investigated and corrective actions enforced.

Amber requirements – variations permitted subject to approved risk analysis and mitigation

- Amber requirements are to be complied with unless an approved variation is in place.
- Amber requirements are presented with an amber sidebar.
- Amber requirements are monitored for compliance.
- Variations can only be approved through the national non-compliance process.
- Non-approved variations will be investigated and corrective actions enforced.

Green guidance – to be used unless alternative solutions are followed

- Guidance should be followed unless an alternative solution produces a better result.
- Guidance is presented with a dotted green sidebar.
- Guidance is not monitored for compliance.
- Alternative solutions should be documented to demonstrate effective control.

Amendment marks

- First document amendments are presented with a single black line to the right of the affected text.
- Second document amendments are presented with a double black line to the right of the affected text.

Ref:	NR/L2/INF/02242/01
Issue:	1
Date:	05 March 2016
Compliance date:	07 June 2016

Issue record

Issue	Date	Comments
1	March 2016	Module replaces NR/L2/INF/02234. This issue contains new information to conform with national standards and reflect best practice.

Compliance

This Network Rail standard is mandatory and shall be complied with by Network Rail and its contractors if applicable from 7th June 2016.

Reference documentation

NR/L1/INF/02232, *Information Security Policy*

NR/L2/INF/02223, *Information Security Classification*

NR/L3/INF/02224, *Sharing Framework for Information*

NR/L3/INF/02231, *Disposal of Records*

NR/L3/INF/02226, *Corporate Records Retention Schedule*

Code of Business Ethics: Available on Connect

Policy on Staff Use of Social Media: Available on Connect

Data Communities: Available on Connect

Disclaimer

In issuing this document for its stated purpose, Network Rail makes no warranties, express or implied, that compliance with all or any documents it issues is sufficient on its own to ensure safe systems of work or operation. Users are reminded of their own duties under health and safety legislation.

Supply

Copies of documents are available electronically, within Network Rail's organisation. Hard copies of this document may be available to Network Rail people on request to the relevant controlled publication distributor. Other organisations may obtain copies of this from an approved distributor.

Ref:	NR/L2/INF/02242/01
Issue:	1
Date:	05 March 2016
Compliance date:	07 June 2016

Contents

1 Purpose	6
2 Scope	6
3 Roles and responsibilities	6
4 Information and information systems	7
4.1 Acceptable use of Network Rail information and information systems	7
4.2 Limited personal use	7
4.3 Unacceptable use of information and information systems	8
5 Access control	9
5.1 Requesting access	9
5.2 Management of passwords	9
5.3 Allocation of passwords	10
6 Network Rail wireless network	11
6.1 Network Rail corporate wireless network	11
6.2 Network Rail guest wireless network	12
7 Devices and equipment	13
7.1 Using corporate devices and equipment securely	13
7.2 Using personal devices and equipment securely	13
7.3 Security controls	13
7.4 Mobile devices	14
7.5 Use of fixed telephones	14
7.6 Use of voicemail	14
7.7 Remote access to Network Rail information systems and services	14
7.8 Removable media	15
7.9 Additional software	15
7.10 Disposal	15
7.11 Leavers	16
7.12 Information ownership	16
8 Email	17
8.1 Acceptable use of email	17
8.2 Receipt of inappropriate email	17
8.3 Spam and phishing emails	18
8.4 External webmail	18
9 Internet and Intranet	19

Ref:	NR/L2/INF/02242/01
Issue:	1
Date:	05 March 2016
Compliance date:	07 June 2016

9.1 Acceptable use of the Internet and Intranet	19
9.2 Social media	19
9.3 Cloud computing	20
10 Monitoring and privacy	20
11 Reporting of security incidents	21

Copyright Network Rail

Ref:	NR/L2/INF/02242/01
Issue:	1
Date:	05 March 2016
Compliance date:	07 June 2016

1 Purpose

Inappropriate use of Network Rail's information and information systems exposes Network Rail to:

- a) security breaches;
- b) compromised network systems and services; and
- c) non-compliance with regulatory requirements.

The implementation of this module contributes to the mitigation of these risks.

2 Scope

This module specifies the acceptable use of Network Rail's information and information systems.

It applies to all Users who have access to Network Rail's information and information systems.

NOTE: Failure to comply with this module might constitute a breach of terms and conditions of employment or contract and can lead to legal or disciplinary action including dismissal or termination of contract. In instances where disciplinary action is required this will be in accordance with the Network Rail Fair Culture process.

3 Roles and responsibilities

Data Community Representative

An individual nominated by a Data Community Owner to act on behalf of the Data Community Owner.

User

Anyone who has access to Network Rail information and information systems including employees, volunteers, contractors, temporary staff, delivery partners including off-shore based and third party suppliers.

External User

A User who is a recognised representative or guest of a Network Rail service provider, consultant, supplier or partner working for or alongside Network Rail, on or off site.

Sponsor

A Network Rail employee who is responsible for the access granted to External User(s) accessing Network Rail's information and information systems.

Ref:	NR/L2/INF/02242/01
Issue:	1
Date:	05 March 2016
Compliance date:	07 June 2016

4 Information and information systems

4.1 Acceptable use of Network Rail information and information systems

Users shall only use Network Rail's information systems:

- a) for business purposes as part of their role; or
- b) for limited personal use.

Users shall use Network Rail information in accordance with NR/L3/INF/02223 Information Classification and Network Rail's *Code of Business Ethics*.

Users shall manage the information in line with NR/L3/INF/02224 Sharing Framework for Information when sharing the information with third parties.

4.2 Limited personal use

By choosing to use Network Rail's information systems for limited personal use, Users accept that their communication and web browsing activities might be monitored.

Limited personal use is determined by the User's line manager.

When using Network Rail information systems users shall:

- a) not knowingly introduce a computer virus or other harmful file to Network Rail information system;
- b) not knowingly circumvent Network Rail security controls;
- c) not use any Network Rail information and information systems classified as Internal, Confidential or Secret for personal use;
- d) not use personal accounts for Network Rail business. This includes Network Rail business related communications, business related attachments, or emails containing Network Rail's information;
- e) not allow personal use to interfere with their normal duties;
- f) engage in activities for financial profit;
- g) not adversely affect the safety, health and wellbeing of themselves and others;
- h) not cause reputational damage to Network Rail; and
- i) not adversely affect Network Rail financially.

Network Rail accepts no responsibility for issues arising from the personal use of Network Rail's information systems, which is undertaken at the User's own risk.