

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

Level 2

Information Security – Acceptable Use of Information and Information Systems

Endorsement and Authorisation

Endorsed by:



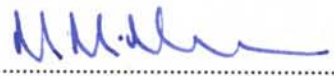
Lucy Cairns, Working Group Chair

Authorised by:

 (Gary Leach)

Gary Leach, Steering Group Chair

Accepted for issue by:



Mick McManus, National Standards Manager

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 2012 Network Rail.

Uncontrolled copy once printed from its electronic source.

Published and Issued by Network Rail, Kings Place, 90 York Way, London. N1 9AG.

NetworkRail

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be to the replacement standard.

Documents
Document Sharing Hub

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

User information

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

Red requirements – *No deviations, could stop the railway*

- **Red requirements shall** always be complied with and achieved.
- Red requirements shall be presented in a red box **with the word “shall” or expressed as a direct instruction**.
- Accountability for the efficacy of red requirements lies with the Professional Head/Standard Owner.
- Red requirements are monitored for compliance.
- Corrective actions shall be enforced if deviations are discovered through functional checks (e.g. engineering verification visits, audit or Operations Self-Assurance).

Amber requirements – *Controlled deviations, approved risk analysis and mitigation*

- **Amber requirements shall** be complied with unless deviation has been approved in advance.
- Amber requirements shall be presented with an amber sidebar **and with the word “shall” or expressed as a direct instruction**.
- Accountability for the efficacy of these requirements lies with the Professional Head/Standard Owner, or their nominated Delegated Authority.
- Amber requirements are monitored for compliance.
- Deviations **may** be permitted. Deviations are approved by the Standard Owner or through existing Delegated Authority arrangements.
- Corrective actions shall be enforced if **non-approved** deviations are discovered through functional checks (e.g. engineering verification visits, audit or Operations Self-Assurance).

Green – *Guidance*

- Guidance is based on good practice. Guidance represents supporting information to help achieve **Red** and **Amber** requirements.
- Guidance shall be presented with a dotted green sidebar **and with the word “should” (usually in notes) or as a direct instruction**.
- Guidance is **not mandatory** and is not monitored for compliance.
- Alternative solutions may be used. Alternative solutions do not need to be formally approved.
- Decisions made by a competent person to use alternative solutions should be backed up by appropriate evidence or documentation.

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

Issue record

Issue	Date	Comments
1	December 2009	First issue as Network Rail standard.
2	March 2012	This issue is raised from a Level 3 to a Level 2 standard and is additionally intended to replace NR/L2/INF/02233, <i>User Requirements</i>. This issue includes a revision of existing content, where required; the content of NR/L2/INF/02233; and further covers removable media, cloud computing, use of the company wireless networks, the storage of personal data in email and the secure use of devices and equipment.

Compliance

This Network Rail standard is mandatory and shall be complied with by Network Rail and its contractors if applicable from 2nd June 2012.

When this standard is implemented, it is permissible for all projects that have formally completed GRIP Stage 3 (Option Selection) to continue to comply with the issue of any relevant Network Rail standards current when GRIP Stage 3 was completed and not to comply with requirements contained herein, unless stipulated otherwise in the scope of this standard.

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*.

Code of Business Ethics: Available on Connect. Owner: Deputy Company Secretary.

Policy on Staff Use of Social Media: Available on Connect. Owner: Head of Digital Marketing.

Internet Access Filtering: Available on Connect. Owner: Information Security Policy Manager.

Line Managers Security Policy: Available on Connect. Owner: Information Security Policy Manager.

Data Communities: Available on Connect. Owner: Information Security Policy Manager.

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

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

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 document from IHS. Tel: 01344 328039.

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

Contents

1 Purpose	6
2 Scope	6
3 Roles and responsibilities	6
4 Definitions	7
5 Information and information systems	9
5.1 Acceptable use of Network Rail information and information systems	9
5.2 Limited personal use	9
5.3 Unacceptable use of information and information systems	10
6 Access control	11
6.1 Requesting access	11
6.2 Management of passwords	11
6.3 Allocation of passwords	12
7 Network Rail wireless network	13
7.1 Network Rail corporate wireless network	13
7.2 Network Rail Guest wireless network	13
8 Devices and equipment	14
8.1 Using corporate devices and equipment securely	14
8.2 Using personal devices and equipment securely	15
8.3 Security controls	15
8.4 Removable media	15
8.5 Additional software	16
8.6 Disposal	16
8.7 Leavers	16
8.8 Information ownership	16
9 Email	17
9.1 Acceptable use of email	17
9.2 External webmail	17
10 Internet and Intranet	18
10.1 Acceptable use of the Internet and Intranet	18
10.2 Social media	19
10.3 Cloud computing	19
11 Monitoring and privacy	20
12 Reporting of security incidents	21

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

1 Purpose

Network Rail relies upon the confidentiality, integrity and availability of Network Rail information. Safety, community relationships or commercial interests could be impacted if Network Rail's information or information systems are compromised or unavailable when required.

2 Scope

This Network Rail standard specifies the acceptable use of Network Rail's information and information systems. It applies to all Network Rail employees and all Users of Network Rail's information and information systems.

It is not applicable to the use of Network Rail's information and information systems made available to the public.

Failure to comply with this standard may 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. Network Rail reserves the right to undertake disciplinary action against any employee breaching the requirements of this standard without a previously agreed exception.

3 Roles and responsibilities

User

Anyone making use of Network Rail's information and information systems, including employees, contractors and third party users of Network Rail's information systems. This excludes the use of Network Rail's information systems made available to the public.

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.

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

4 Definitions

For the purpose of this standard, the definitions in NR/L1/INF/02232, *Information Security Policy* and the following apply.

adware

free software supported by advertising messages

Bluetooth

a short range wireless technology

cloud computing

software and information management services hosted via the Internet and external to Network Rail, e.g. Hotmail, Demographix, SurveyMonkey, Slideshare, YouSendIt, Youtube, Flickr, Google Docs and Amazon Web Services

corporate wireless network access

access that enables wireless network access to the Internet and any authorised internal resources

freeware

software that is available for free, usually over the Internet

Guest wireless network access

access that enables wireless network access to the Internet and VPN only

information

documentation, data or evidence of activities, decisions and transactions, whether generated formally or informally

information systems

systems in place to manage the processing and storage of information, including, but not limited to, computer equipment, software, operating systems, telecommunications and storage media

malware

malicious software in the form of computer viruses, worms, Trojan horses, spyware, etc

personal data

data about an identifiable individual

personal device

personally owned device, e.g. smartphone or tablet computer

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

removable media

removable data storage, e.g. USB data storage devices (including personal devices), external hard drives, DVDs, CDs and memory cards

sensitive information

Network Rail's information that is classified as Secret or Confidential

shareware

copyrighted software that is available free of charge on a trial basis, usually with the condition that users pay a fee for continued use and support.

social media

Internet and mobile-based technologies for social interaction, e.g. MySpace, Facebook and Twitter

Virtual Private Network (VPN)

logical connection that is encrypted and uses the Internet to connect back to a corporate network or website

wired network

communication network accessed via physical network cabling

wireless network

communications network accessed via wireless signalling technologies

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be to the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

5 Information and information systems

5.1 Acceptable use of Network Rail information and information systems

Users may use Network Rail's information systems:

- a) for business purposes as part of a User's role;
- b) for limited personal use.

Users shall use Network Rail's information only for Network Rail business purposes and in compliance with Network Rail's *Code of Business Ethics*.

When information needs to be shared between Network Rail and third parties, the process by which access to Network Rail's information is controlled and managed is defined in NR/L3/INF/02224, *Sharing Framework for Information* and in line with Data Communities requirements and guidance. The access to and sharing of information is governed according to NR/L3/INF/02223, *Information Security Classification*.

Users shall comply with NR/L3/INF/02223 and treat information according to its four security classifications:

- Public
- Internal
- Confidential
- Secret.

5.2 Limited personal use

By choosing to use Network Rail's information systems for limited personal use, Users shall accept that due to monitoring activities, communications and information cannot be considered as always being private.

Limited personal use of Network Rail's information systems shall:

- a) not be applicable to Network Rail information classified as Internal, Confidential or Secret;
- b) not apply to databases or applications containing Network Rail's information;
- c) not interfere with normal duties;
- d) be within your line manager's discretionary recommendations, which if unclear, should be clarified with your line manager before personal use is undertaken;
- e) be on a non-business and not-for-profit basis;
- f) not adversely affect the safety, health and wellbeing of yourself and others;
- g) not cause reputational damage to Network Rail; and
- h) not adversely affect Network Rail financially.

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

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.

5.3 Unacceptable use of information and information systems

Unacceptable uses of Network Rail information and information systems shall include use in any way that is, or may be considered:

- a) abusive;
- b) offensive or obscene, including pornographic images or materials, or other images text or materials that are insensitive or offensive, including but not limited to:
 - 1) race;
 - 2) ethnicity;
 - 3) nationality;
 - 4) religion;
 - 5) religious beliefs and/or other beliefs;
 - 6) political opinions views;
 - 7) age;
 - 8) disability;
 - 9) sexist;
 - 10) marital status;
 - 11) gender; or
 - 12) sexual orientation.
- c) sexually explicit;
- d) discriminatory;
- e) threatening;
- f) defamatory;
- g) financially or commercially detrimental to Network Rail;
- h) illegal;
- i) unethical; or
- j) excessive.

Users shall not use Network Rail's information and information systems for business purposes that are not defined as part of a User's role and shall follow Network Rail's *Code of Business Ethics* in all business dealings and relationships.

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

6 Access control

6.1 Requesting access

Users requiring access to Network Rail's information systems shall submit their access request to the Network Rail IT Helpdesk.

Access will only be granted upon approval from the relevant authoriser.

Control arrangements are in place:

- a) to restrict access to Network Rail's information systems to authorised Users only;
- b) to provide authorised Users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority; and
- c) for Users to be individually accountable for all actions undertaken via these access privileges.

6.2 Management of passwords

Users shall authenticate themselves by using their username and password as login credentials. Users shall:

- a) keep their passwords completely private;
- b) not share them;
- c) make them hard to guess; and
- d) not record them where others can access them.

Users shall be responsible and accountable for any actions/activities that are carried out under their User account on any Network Rail information system.

Password composition for User accounts on Network Rail's corporate IT network (Microsoft Active Directory or AD) will require the following password constraints as a minimum:

- a) be at least eight characters long;
- b) contain at least one upper case letter;
- c) contain at least one non alphabetic character, e.g. number or symbol;
- d) contain lower case letters;
- e) not contain the username;
- f) not be the same as any of the five recent passwords; and
- g) be changed every 90 days.

Password conditions for other information systems may vary.

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.

Ref:	NR/L2/INF/02234
Issue:	2
Date:	03/03/2012
Compliance date:	02/06/2012

To protect Network Rail's information from unauthorised access, User accounts on Network Rail's corporate IT network become locked after five incorrect login attempts and inactive sessions are secured either by locking the sessions and requiring re-authentication or by timing out the session connection after a defined period of inactivity.

6.3 Allocation of passwords

Any User requiring a password reset shall contact the Network Rail IT Helpdesk. If a User suspects that their or another User's password has been compromised, they shall report this to the Helpdesk immediately.

Users requesting new passwords or password changes will be verified and confirmed before a password is issued and before User access controls are reset or unlocked. For sensitive accounts (where access is granted to personal data or secret information), requests may undergo additional verification.

Network Rail follows a process for the secure allocation of passwords, including:

- a) Users' passwords being communicated in a secure manner, e.g. by phone or by internal email;
- b) passwords not being communicated along with usernames;
- c) forced password change upon initial login; and
- d) passwords for generic accounts only being communicated to Users requiring access to carry out their job function.

This standard should only be used for reference to ensure 'The Control of Risk' until the compliance date of its replacement standard is reached, upon which this standard will be withdrawn. The development of all new processes and procedures should be in line with the replacement standard.