

**R Systems International Ltd.**

C-40, Sector 59

Noida 201 307 (U.P.), India

<http://www.rsystems.com/>

**DocumentId.: ISguide VersionNo.: 1.0**

**Releasedon: 22/05/06**

**R Systems International Ltd.**

C-40, Sector 59

Noida 201 307 (U.P.), India

<http://www.rsystems.com/>

**End User Guidelines**

**Document Id. : ISGuide003 VersionNo. : 3.2 Releasedon :31/07/19**

*This document of R Systems International Ltd. is for internal circulation. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any from or by any means – recording, photocopying, electronics and mechanical without prior written permission of R Systems International Ltd.*

# DOCUMENT CONTROL SHEET

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Document History** | | | | | | |
| **Ver. No.** | | **Release Date** | **DCR**  **Ref.** | **Description of Change** | **Authored/ Revised**  **By** | **Reviewed By** | **Approved By** |
| 1.0 | | 09/06/06 | DCR/0 02 | Final release | QA Group | ISMS  Forum | CISO |
| 1.1 | | 14/01/09 | DCR/0 18 | Updation of  temporary access card process | QA Group | ISMS  Forum | CISO |
| 2.0 | | 01/06/09 | DCR/IS MS/038 | ISMS periodic review | QA Group | ISMS  Forum | CISO |
| 2.1 | | 04/03/11 | DCR/IS MS/081 | Periodic Review | QAG – ISMS | Prabhas Dash | CISO |
| 2.1 | | 01/06/12 | NA | ISMS periodic review | ISMS  Team | Manager QAG | CISO |
| 2.2 | | 09/08/12 | DCR/IS MS/105 | Classification changed to Internal | ISMS  Team | Manager QAG | CISO |
| 2.3 | | 09/05/13 | DCR/IS MS/107 | Changes done as per PCIDSS  requirements | ISMS  Team | Manager QAG | CISO |
| 2.4 | | 01/01/14 | DCR/IS MS/112 | RSI Logo Updated | ISMS  Team | Manager QAG | CISO |
| 2.4 | | 15/06/15 | DCR/IS MS/122 | Periodic Review | ISMS  Team | Manager QAG | CISO |
| 2.5 | | 20/05/16 | DCR/IS MS/132 | Annual Review Year 2016- Helpdesk link updated, Section 8.2.1 & 8.2.2  updated | ISMS  Team | Sr. Manager QAG | CISO |
| 3.0 | | 18/07/17 | DCR/IS MS/136 | Annual Review-  Section 3 Admin Guidelines | ISMS  Team | Sr.  Manager QAG | CISO |
| 3.1 | | 18/07/18 | DCR/IS MS/141 | Annual Review- 21/06/18,  Section 4 Computing Guidelinesrelated  to GDPRupdated | ISMS  Team | Sr. Manager QAG | CISO |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3.2 | 31/07/19 | DCR/IS MS/144 | Annual Review- 25/07/19.  Removed following line from 10.3 &  10.4 “Hardcopies of docs to be stamped in blue/red”  Section 5 updated to include password history  requirement | ISMS  Team | Sr. Manager QAG | CISO |

### Notes:

* *Only controlled hardcopies of the document shall have signatures onthem.*
* *This is an internal document. Unauthorized access or copying isprohibited.*
* *Uncontrolled when printed unless signed by approvingauthority.*



© R Systems International Limited 2019

# Table of Contents

1. [Purpose 4](#_TOC_250017)
2. [Scope 4](#_TOC_250016)
3. [AdminGuidelines: 4](#_TOC_250015)
4. [ComputingGuidelines: 5](#_TOC_250014)
5. [PasswordUsage Guidelines: 6](#_TOC_250013)
6. [GeneralGuidelines: 6](#_TOC_250012)
7. [IPR, Data Security, Confidentiality& Privacy 7](#_TOC_250011)
8. [AcceptableUse 7](#_TOC_250010)
   1. [GeneralUse 7](#_TOC_250009)
      1. [Security andProprietary Information 7](#_TOC_250008)
   2. [UnacceptableUse 8](#_TOC_250007)
      1. [System andNetwork Activities 8](#_TOC_250006)
      2. [Email andCommunications Activities 9](#_TOC_250005)
9. [Information Labelling, Handling &ExchangeGuidelines 10](#_TOC_250004)
   1. [Public 10](#_TOC_250003)
   2. [Internal 11](#_TOC_250002)
   3. [Restricted 11](#_TOC_250001)
   4. [Confidential 11](#_TOC_250000)

## End User Guidelines

## Purpose

To establish guidelines for all employees and end-users of RSI, to aid enforce them organization-wide information security.

## Scope

These guidelines are applicable to all the employees, contractors & third party personnel at RSI.

## AdminGuidelines:

* Users should display their own identification cards (Proximity Card)prominently.
* Users should use their own Proximity Card to get access tofacilities.
* Incase an employee forgets to bring their ID card, Security Supervisor will ask the respective Manager / Team Leader to come to the Security Gate to sign in the issue register for issuing a temporary access card to the employee for the day. For more details on the process of issuing temporary access card please refer to section 3.1.1 in Administration Guidelines(ISGuide002).
* Users should not, in any case tail gate or gain access to a facility to which they are not authorized to. In case there is a business reason to access a particular facility/floor/server room then an Approval is needed from the Business head of the project/function.
* Users should report all breach of security incidents to administration on IPLC ext. 311111, or<http://helpdesk.india.rsystems.com/>or IT Helpdesk & Physicallocations.
* Users should cooperate with security team in frisking of usersbelongings
* Users should follow standard operating procedures that are stipulated from time-to- time.
* Users should proactively handover the keys of the drawer or cabin at the time of shifting from one seat toanother.
* Employees should not use the area near DG sets forsmoking.
* Ensure that users are aware of the emergency/fireexits.
* The ID & Access Card is a card issued as standard identification of personnel, employees etc. There are 5 different kinds of access cards used inRSI

**Signature: **

**Date Of Joining: 07-11-2022**

**BLUE** – For Employees **RED** – For Visitors **YELLOW**– For ThirdParty

**Sky BLUE** – For Temporary Access Card

**Violet -** For Client withclip.

In RSI access cards are mandatory and should be carried by every employee all the time either entering the floors or leaving.

In case employee forgets to bring ID cards is required to take permission from his/her immediate superior and make an endorsement in the incoming/outgoing register & get Temporary access card at thegate.

Employees coming on week-ends/holidays are requested to carry their access cards

## ComputingGuidelines:

* Users are expected to keep their passwords secure and confidential. Giving your password to others is explicitlyforbidden.
* Users should not store personally-identifiable information about others on their PC, even though it may be convenient to doso.
* Users should abide by all applicable Acceptable Use Guidelines (mentioned below in the document). Users should log off or Lock PC when leaving for theday.
* Users should not use removable media disks e.g. floppy drive and CD-Writer except where specifically authorized by reporting PAM/Manager &CISO.
* Kazaa, Gnutella, and any other form of File Sharing or peer-to-peer applications are strictlyforbidden.
* Users should not use unauthorized software. RSI uses software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by employee. Reports of attempted access should be scrutinized by technology group on a regularbasis.
* Information and data stored on Laptop or portable computers be backed upregularly.
* Only authorized equipments should be taken outside the RSI premises i.e. laptop users must sign an undertaking and for other official equipment gate pass must be issued.
* Do not use any unauthorizedsoftware.
* Should not leave unattended diskettes / tapes /papers containing information classified asconfidential.
* All critical data/information should be stored on shared location available at SAN boxes.
* Should not attempt to gain access without proper authorization to a computing system ornetwork.
* All users should check for version update of System Center Endpoint protection antivirus signature, if found an old version (older than two days than the current date) it should be reported to Networkteam.
* Report all IT related issues to the IT helpdesk at<http://helpdesk.india.rsystems.com/> or at IPLC Extn.: 311111 or IT Helpdesk & Physicallocations.
* Any user working on any European Union Data, shall abide GDPR compliance and should not store any PII given by any respectivecustomer.

**Signature: **

**Date Of Joining: 07-11-2022**

## Password UsageGuidelines:

* Users should not use their user id as password in anyform;
* Users should not use their first, middle or last name as password, family orpet names or nicknames;
* Password should not be shared with anyone till the time required to fulfill business purpose.
* Information easily obtained about them e.g. license plate, telephone number, date of birth, employee or payroll number should not be used aspasswords;
* All digits or the entire sequence of single letter should not be used (example: common character sequences like 1234567, abcdefg) as passwords;and
* Password string length should be minimum 8characters.
* Users will be prohibited from re-using the last 4 previously usedpasswords.
* All users must change the password at the firstlogin
* All users should change their passwords within every 42days.

Password selection should adhere to the following guidelines:

* The password should contain the following characterclasses:
  + Lower casecharacters
  + Upper casecharacters
  + Numbers

o Special characters (e.g. @#$%^&\*()\_+|~-=\`{}[]:";'<>/etc)

* The password is not a word found in a dictionary (English orforeign)
* The password is not a common usage word suchas:
  + Names of family, pets, friends, co-workers, fantasy characters,etc.
  + Computer terms and names, commands, sites, companies, hardware, software.
  + The words "rsystems", "sanjose", "sanfran" or anyderivation.
  + Birthdays and other personal information such as addresses and phone numbers.
  + Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321,etc.
  + Any of the above spelledbackwards.
  + Any of the above preceded or followed by a digit (e.g., secret1,1secret)
* Passwords should never be written down or stored on-line.

## GeneralGuidelines:

* Clear Desk and Clear Screen should bemaintained.
* All documents of confidential nature should be shredded when no longer required. The document owner must authorize or initiate thisdestruction.
* Eatable/drinks should not be carried to theworkstation.
* Music, movies & Games should not be played, on thesystem/Laptop
* People roaming around the facility without ID cards should bechallenged.
* Cameras and audio recording devices should not be allowed into the workarea.

**Signature: **

**Date Of Joining: 07-11-2022**

* Server room access is restricted to authorized personnel only and users should not attempt to enter such rooms to which they have not been providedaccess.

## IPR, Data Security, Confidentiality &Privacy

RSI users should be responsible for ensuring the confidentiality and appropriate use of organizational and customer data/information to which they are given access, ensuring security of the equipment where such information is held or displayed, and abiding by related privacy rights concerning the use and release of personal information, as required by law & RSI policies, including Confidentiality & Non DisclosureAgreement.

Standard Process on IPR Protection (Qproc040) is made available on RSI Intranet site as part of QMS.

Copyright law should apply to all forms of information, including electronic communications, and violations are prohibited. Infringements of copyright laws include, but are not limited to, making unauthorized copies of any copyrighted material (including software, text, images, audio, and video), and displaying or distributing copyrighted materials over computer networks without the author's permission except as provided in limited form by copyright fair use restrictions.

## Acceptable Use

#### GeneralUse

* RSI’s network administration should provide a reasonable level of privacy to the users for business purposes, users should be aware that the data they create on the corporate systems’ remains the property ofRSI.
* Responsibility for exercising good judgment regarding the reasonableness of personal use should be that of the user of the asset. Individual should be responsible for the use of Internet/Intranet/Extranetsystems.
* Laptop users should agree to take shared responsibility for the security of their laptop and the information it contains as per the Communication and Operations Management Policy (ISPolicy033). They need to sign a Laptop UndertakingForm.
* For security and network maintenance purposes, authorized individuals within RSI should monitor equipment; systems and network traffic at any time and reviewthem.

#### Security and ProprietaryInformation

* The user interface for information contained on Internet/Intranet/Extranet-related systems and hardcopies should be classified as Confidential, Restricted, Internal or Public, as defined by Asset Management Policy(ISPolicy031).
* Authorized users should be responsible for the security of their passwords and accounts. System and user level passwords should be changed after a fixed duration oftime.
* All PCs, laptops and workstations should be secured with a passwordprotection.
* Information contained on portable computers is vulnerable, special care should be exercised by their user. For more details refer Laptop Securitypolicy.

**Signature: **

**Date Of Joining: 07-11-2022**

* Postings by employees from a RSI email address should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of RSI, unless posting is in the course of businessduties.
* All hosts used by the employee that are connected to the RSI Internet/Intranet/Extranet, whether owned by the employee or RSI, should be continually executing approved virus-scanning software with a current virus database.
* Employees should take caution while opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horsecode.
* In case an Asset (Laptop, Hardware Equipment, etc) is lost or stolen appropriate authorities should be intimated as per the Information Security Incident Management Policy(ISPolicy036).
* Information should not be left unattended at Photocopiers, Printers, Fax machines, etc
* The custodian of any form of information storage media should be responsible for the asset as per the Asset Management Policy(ISPolicy031).
* No personal electronic & computing devices are allowed on the floors compliant to PCI DSSstandard.

#### UnacceptableUse

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of RSI authorized to engage in any activity that is illegal under law while utilizing RSI-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

#### System and NetworkActivities

The following activities should be strictly prohibited, with no exceptions:

* Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use byRSI.
* Unauthorized copying, scanning of copyrighted material should be prohibited. Laptop users should ensure they comply with data copyrightrequirements.
* Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal and appropriate management should be consulted prior to export such material inquestion.
* Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.). Installation of unlicensed or malicious software on thelaptops.
* Revealing account password and allowing use of account by unauthorized users. This includes family and other household members when work is being done at home.

**Signature: **

**Date Of Joining: 07-11-2022**

* Using RSI computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
* Making fraudulent offers of products, items, or services originating from any RSI account.
* Making statements about warranty, expressly or implied, unless it is a part of normal jobduties.
* Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for maliciouspurposes.
* Port scanning or Network scanning is expressly prohibited unless authorized by Head IT Infrastructure &CISO.
* Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty is prohibited.
* Circumventing user authentication or security of any host, network oraccount.
* Interfering with or denying service to any user other than the employee's host (for example, denial of serviceattack).
* Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via theInternet/Intranet/Extranet.
* Providing information about, or lists of, RSI employees to parties outsideRSI.
* Use of such software/technique which bypass RSI’s Grouppolicy.
* All the employees are expected to use only the approved software and hardware resources. The list of all the approved software and hardware resources is available with the AVP IT Systems, which can be available from him onrequest.
* Operating Systems updates pushed by IT Systems Team shall be pushed manually by employee itself on regularintervals.
* External devices (CD drive, USB ports, Floppy drive etc.) shall be disabled from individual desktops used by employees unless explicitlypermitted
* Access to website like YouTube, Facebook etc. those are unwanted and utilizes network bandwidth are strictly prohibited. Documented approval will be sought in case there is an exceptional requirement withinproject/process.
* Only domain logins are allowed in RSI environment, no local user login is permissible.

#### Email and CommunicationsActivities

The following activities should be strictly prohibited, with no exceptions:

* Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (emailspam).
* Any form of harassment via email, telephone or paging, whether through language, frequency, or size ofmessages.

**Signature: **

**Date Of Joining: 07-11-2022**

* Unauthorized use, or forging, of email headerinformation.
* Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collectreplies.
* Creating or forwarding "chain letters" or other "pyramid" schemes of anytype.
* Use of unsolicited email originating from within RSI's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by RSI or connected via RSI'snetwork.
* Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroupspam).
* Usage of phones, fax, or other communication equipments other than operational and functional requirement of thebusiness.
* Storage of unsolicited email messages in publicfolders.
* Usage of Public Email like Gmail, Yahoo Mail etc are strictly prohibited. Documented approval will be accorded in case there is an exceptional requirement within project/process.

## Information Labelling, Handling & ExchangeGuidelines

Guidelines for handling, processing, storing, and communicating information consistent with its classification are:

* Handling and labeling of all media should indicate its classification level i.e. Restricted, Confidential, Internal orPublic
* Spooled data awaiting output( Printing or Photocopying) should be protected to a level consistent with itssensitivity;
* The distribution of data should keep to a minimum and should be accessible to authorized persons who require them for businessneeds.
* Distribution list and List of authorized person should be reviewedquarterly.
* System documentation should be storedsecurely.
* Sensitive or critical information should not be left over printing facilities, e.g. copiers, printers, and facsimile machines, as these may be accessed by unauthorized personnel;
* Automatic forwarding of electronic mail to external mail addresses should not be allowed;
* Messages containing sensitive information should not be left on voice mail since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result ofmisdialing;
* Media containing sensitive or critical information should be protected against unauthorized access, misuse or corruption during transportation beyond an RSI’s physical boundaries. Only authorized persons should carry these media to the desireddestinations.
* Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers’ specifications.

Information should be classified and exchanged according to their criticality. Following should be considered as per sensitivity of information/data, but should not be limited to:

### Public

* General information and organizational brochure should be considered aspublic.

**Signature: **

**Date Of Joining: 07-11-2022**

* Information pertaining to RSI which is available on www domain could be accessed byanyone.
* Public information should be made available throughInternet/E-mails.
* Softcopies of the document should be labeled as “Public” and label should be in the centre of theheader.
* Hard/Softcopies with no label should be considered as“Public”.
* Hard copies of the “Public” documents should not bestamped.
* Hardcopies of documents should be destroyed off after expiration of defined retention period. Electronic data/information should be off-loaded from intranet/internet and should be backed up ifrequired.

### Internal

* Information of proprietary nature which is meant for all the employees of R Systems such as – Policies, Guidelines, Forms, Handoutsetc.
* Access to information labeled “Internal” should be given to authorized persons within R Systems and is for circulation within theorganization.
* Internal Information/Data should be made available through Intranet/SVN/ E-mails to employees and to third party personnel with a business need toknow.
* Softcopies of the document should be labeled as “Internal” and label should be in the centre of theheader.
* Hard copies of the “Internal” documents should be labeled as“Internal”.
* Hardcopies of documents should be shredded off after expiration of defined retention period. Electronic data/information should be backed up and stored in safe environment for defined retentionperiod.

Media containing obsolete internal information/data should be destroyed/ formatted. Information asset owner should initiate the disposal.

### Restricted

* All information of proprietary nature - procedures, operational work routines, project plans, designs and specifications that define the way in which RSI operates should be considered as“Restricted”.
* Access to information labeled “Restricted” should be given to authorized persons with a business need to know and is for circulation within theorganization.
* Restricted Information/Data should be made available through Intranet/SVN/ E-mails to employees and to third party personnel with a business need toknow.
* Softcopies of the document should be labeled as “Restricted” and label should be in the centre of theheader.
* Hardcopies of documents should be shredded off after expiration of defined retention period. Electronic data/information should be backed up and stored in safe environment for defined retentionperiod.

Media containing obsolete restricted information/data should be destroyed/ formatted. Information asset owner should initiate the disposal.

### Confidential

**Signature: **

**Date Of Joining: 07-11-2022**

* All information regarding Business, financial, Trade secrets, marketing, operational, technical and customer /client information etc. should be considered as “Confidential”.
* Access to information labeled “Confidential” should be given to authorized persons with a business need to know and relevant level of physical and logical access should beprovided.
* Softcopies of the document should be labeled as “Confidential” and label should be in the centre of theheader.
* Hardcopies of documents should be shredded off after expiration of defined retention period. Electronic data/information should be backed up and stored in safe environment.
* Media containing “Confidential” information/data which is no longer required should be destroyed/ formatted. Information asset owner should initiate thedisposal.

**Signature:**  ****

**Date Of Joining: 07-11-2022**