Caring - Innovating - Transforming

Employee No.
(To be filled in by HR)

Passport Size Photograph

EMPLOYMENT FORM

EMPLOYEE DETAILS

First Name	Gaurav	**Middle Name**		**Last Name**	Gupta
Date Of Birth (as per records)	10-Dec-82 (dd/mmm/yy)	**City & State Of Birth**	Agra,Uttar Pradesh		
Date Of Birth (Social- if different than above)	(dd/mmm/yy)		**Total Experience**	14 (Years)	
Nationality	Indian		**Relevant Experience**	11 (Years) 0 (Months)	

PERSONAL DETAILS

Gender	Male	**Marital Status**	Married	**Spouce's Name**	Reetika Gupta
Father Name	Shri Krishna Kaushal	**Mother's Name**	Pushpa Kaushal	**Blood Group**	O+
Physically Handicapped	No	**Religion**	Hindu	**Reservation Category (General/SC/ST/ OBC)**	General
Personal Email ID	gauravgupta1012@ gmail.com	**Alternate Email ID**		**Marriage Anniversary**	23-Feb-12
Passport Details (No.)		**Expires On**		**Voter Card number**	
Social Security Number		**Aadhaar Number**	479488478745	**Ongoing Maternity**	NA

Medical Details

Name	Date Of Birth	Gender	Age
Gaurav Gupta	10-Dec-1982	M	39
Reetika Gupta	28-Nov-1984	F	37
Vihaan Gupta	30-Aug-2014	M	8
Pushpa Kaushal	20-Jul-1955	F	67
Shri Krishna Kaushal	10-Jul-1946	M	76

FAMILY DETAILS (Parents/Spouse/Child)

S.No.	Name Of Dependent	Gender	Date Of Birth	Relationship
1	Reetika Gupta	Female	28-Nov-84	Wife
2	Vihaan Gupta	Male	30-Aug-14	Son
3	Pushpa Kaushal	Female	20-Jul-55	Mother
4	Shri Krishna Kaushal	Male	10-Jul-46	Father

ADDRESS DETAILS

Present Address			Permanent Address		
House No.	C-2506		**House No.**	C-2506	
Street	JM Florence		**Street**	JM Florence	
City			**City**		
State	Uttar Pradesh		**State**	Uttar Pradesh	
Country	India		**Country**	India	
Pin Code	201306		**Pin Code**	201306	
	Mobile	**Phone No.**		**Mobile**	**Phone No.**
Contact No.	9811164837		**Contact No.**	9811164837	

ACADEMIC QUALIFICATIONS

(Photostate Copies Of Original Degree/Certificates/Transcripts required).

Examination Passed	Duration		University	College	Division
	From	To			
BCA	2001	2003	Dr. Bhim Rao Ambedkar University: Agra University, Agra	Raja Balwant Singh College	1st
Senior secondary	2000	2000	CBSE	Kendriya Vidyalaya No.1 AFS Agra	2nd
Matriculation	1998	1998	CBSE	Kendriya Vidyalaya No.1 AFS Agra	2nd
MCA	2004	2007	Visveswaraiah Technological University, Belgaum	M.S. Ramaiah Institute of Technology	1st

CERTIFICATE/TRAININGS

Name of Certification/Training	Duration		Certificate ID
	Completed Date	Valid Upto	
-			

DETAILS OF PREVIOUS EMPLOYMENT *(if Any)*

Name of Employer	Joining Date (dd/mm/yy)	Leaving Date (dd/mm/yy)	Designation	Reporting Manager	CTC	Reason For Leaving
HCL Technologies	13-Mar-14	04-Nov-22	TEST LEAD		774496.00	
ONEFORCE SOLUTIONS PVT LTD	24-Jan-11	24-Apr-11	Associate consultant testing		350000.00	
OnMobile Global Limited	05-May-08	21-Jan-11	APPLICATION DEVELOPER		300000.00	
GetIt Infomedia	23-Jul-12	12-Mar-14	Senior Software Testing Engineer		516816.00	
Knowlarity Communications Pvt. Ltd	25-Apr-11	30-Jun-12	QA ENGINEER		412014.00	

REFERENCES

(Please mention names of seniors you had worked with in your previous organizations)

Name	Organisation Name & Location	Tel No. (Off./Personal)	Email id	Relationship with Applicant at the time of working
Avishek Ranjan	HCL NOIDA	8709573959	avishekranjan1909@gmail.com	Colleauge

Employment Verification

Name of HR	Geetha	**Email ID**	GEETHALAKSHMI_S@HCL.COM
Mobile/Landline No.	8940082543	**Address and Location**	Noida , sec 60 HCL Office

Awards

Title	Organization Name and Location

EMERGENCY

(People to be contacted at the time of Emergency)

Name	Mobile No.	Address	Relationship
Reetika Gupta	8860417412	JM Florence , C2506 , Greater Noida west	Wife

Have you ever been involved in any legal case? If yes, mention whether civil or criminal.

Give Details

Empty

I hereby undertake that I shall inform the company in case there is any legal/criminal case filed against me.

LANGUAGE KNOWN

Languages	Read	Speak	Write
Hindi	Yes	Yes	Yes
English	Yes	Yes	Yes

Extra-Curricular activities / Hobbies

MEDICAL INSURANCE

Y ☐ N ☑

Please furnish following details if you have one.

Name of the Company with which insured.

Any other information that you would like to provide.

Please mention chronic medical ailment you suffer from (if any)

I hereby declare that if the above information given by me is found untrue at any time/stage during my tenure of employment, I shall be liable to immediate dismissal from my services without any notice or compensation whatsoever.

Signature of the Applicant

_____

Background Screening Form	
Employee Code	
Employee Name	
Father's Name	
DOJ	
Date of Birth	
Contact No.	
Marital Status	
Address Details	
Address Type	Present [ ] Permanent [ ]
House No.	
Street	
City	
State	
Country	
Postal Code	
Landline No.	
Mobile No.	
Past Employement	
Employee ID	
House No.	
Employer	
Address	
Designation	
From Date	
To Date	

R Systems International Ltd.
C-40, Sector 59
Noida 201 307
(U.P.), India
http://www.rsystems.com/

End User Guidelines

Document Id. : ISguide003

Version No. : 2.4

Released on : 15/06/15

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/002**	**Final release**	**QA Group**	**ISMS Forum**	**CISO**
1.1	**14/01/09**	**DCR/018**	**Updation of temporary access card process**	**QA Group**	**ISMS Forum**	**CISO**
2.0	**01/06/09**	**DCR/ISMS/038**	**ISMS periodic review**	**QA Group**	**ISMS Forum**	**CISO**
2.1	**04/03/11**	**DCR/ISMS/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/ISMS/105**	**Classification changed to Internal**	**ISMS Team**	**Manager QAG**	**CISO**
2.3	**09/05/13**	**DCR/ISMS/107**	**Changes done as per PCI DSS requirements**	**ISMS Team**	**Manager QAG**	**CISO**
2.4	**01/01/14**	**DCR/ISMS/112**	**RSI Logo Updated**	**ISMS Team**	**Manager QAG**	**CISO**
2.4	**15/06/15**	**DCR/ISMS/122**	**Periodic Review**	**ISMS Team**	**Manager QAG**	**CISO**

Notes :

- Only controlled hardcopies of the document shall have signatures on them.
- This is an internal document. Unauthorized access or copying is prohibited.
- Uncontrolled when printed unless signed by approving authority.

Table of Contents

End User Guidelines

1. Purpose

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

2. Scope

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

3. Admin Guidelines:

- Users should display their own identification cards (Proximity Card) prominently.
- Users should use their own Proximity Card to get access to facilities.
- 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://tickets.india.rsystems.com/helpdesk, or IT Helpdesk & Physical locations .
- Users should cooperate with security team in frisking of users belongings
- 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 to another.
- Employees should not use the area near DG sets for smoking.
- Ensure that users are aware of the emergency/fire exits.
- The ID & Access Card is a card issued as standard identification of personnel, employees etc. There are 5 different kinds of access cards used in RSI

BLUE	----	For Employees
RED	----	For Visitors
YELLOW	----	For Third Party
GREEN	----	For Housekeeping
Sky BLUE	----	For Temporary Access Card

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 an Temporary access card at the gate.
Employees coming on week-ends/holidays are requested to carry their access cards

4. Computing Guidelines:

- Users are expected to keep their passwords secure and confidential. Giving your password to others is explicitly forbidden.
- Users should not store personally-identifiable information about others on their PC, even though it may be convenient to do so.
- Users should abide by all applicable Acceptable Use Guidelines (mentioned below in the document). Users should log off or Lock PC when leaving for the day.
- 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 strictly forbidden.
- 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 regular basis.
- Information and data stored on Laptop or portable computers be backed up regularly.
- 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 unauthorized software.
- Should not leave unattended diskettes / tapes /papers containing information classified as confidential.
- 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 or network.
- 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 Network team.
- Report all IT related issues to the IT helpdesk at
- http://tickets.india.rsystems.com/helpdesk or at IPLC Extn.: 311111 or IT Helpdesk & Physical locations.

5. **Password Usage Guidelines:**

- Users should not use their user id as password in any form;
- Users should not use their first, middle or last name as password, family or pet 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 as passwords;
- 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 8 characters.
- All users must change the password at the first login
- All users should change their passwords after every 42 days.

  Password selection should adhere to the following guidelines:
- The password should contain the following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Special characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- The password contains minimum eight or more than eight characters
- The password is not a word found in a dictionary (English or foreign)
- The password is not a common usage word such as:
  - 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 any derivation.
  - 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 spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

- Passwords should never be written down or stored on-line.

6. **General Guidelines:**

- Clear Desk and Clear Screen should be maintained.
- All documents of confidential nature should be shredded when no longer required. The document owner must authorize or initiate this destruction.
- Eatable/drinks should not be carried to the workstation.
- Music, movies & Games should not be played, on the system/Laptop
- People roaming around the facility without ID cards should be challenged.
- Cameras and audio recording devices should not be allowed into the work area.
- Server room access is restricted to authorized personnel only and users should not attempt to enter such rooms to which they have not been provided access.

7. 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 Disclosure Agreement.

IPR Training: 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.

8. Acceptable Use

8.1 *General Use*

- 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 of RSI.
- 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/Extranet systems.
- 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 Undertaking Form.
- For security and network maintenance purposes, authorized individuals within RSI should monitor equipment; systems and network traffic at any time and review them.

8.1.1 *Security and Proprietary Information*

- 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 of time.
- All PCs, laptops and workstations should be secured with a password protection.
- Information contained on portable computers is vulnerable, special care should be exercised by their user. For more details refer Laptop Security policy.
- 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 business duties.
- 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 horse code.
- 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 DSS standard.

8.2 *Unacceptable Use*

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.

8.2.1 System and Network Activities

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 by RSI.
- Unauthorized copying, scanning of copyrighted material should be prohibited. Laptop users should ensure they comply with data copyright requirements.
- 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 in question.
- 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 the laptops.
- 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.
- 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 job duties.
- 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 malicious purposes.
- 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 or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- 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 the Internet/Intranet/Extranet.

- Providing information about, or lists of, RSI employees to parties outside RSI.
- Use of such software/technique which bypass RSI's Group policy.
- 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 GM Systems, which can be available from him on request.

8.2.2 *Email and Communications Activities*

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 (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
- 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's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Usage of phones, fax, or other communication equipments other than operational and functional requirement of the business.
- Storage of unsolicited email messages in public folders.

9. Information Labelling, Handling & Exchange Guidelines

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 or Public
- Spooled data awaiting output(Printing or Photocopying) should be protected to a level consistent with its sensitivity;
- The distribution of data should keep to a minimum and should be accessible to authorized persons who require them for business needs.
- Distribution list and List of authorized person should be reviewed quarterly.
- System documentation should be stored securely
- 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 of misdialing;
- 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 desired destinations.

- 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:

10.1 Public

- General information and organizational brochure should be considered as public.
- Information pertaining to RSI which is available on www domain could be accessed by anyone.
- Public information should be made available through Internet/E-mails.
- Softcopies of the document should be labeled as "Public" and label should be in the centre of the header.
- Hard/Softcopies with no label should be considered as "Public".
- Hard copies of the "Public" documents should not be stamped.
- 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 if required.

10.2 Internal

- Information of proprietary nature which is meant for all the employees of R Systems such as – Policies, Guidelines, Forms, Handouts etc.
- Access to information labeled "Internal" should be given to authorized persons within R Systems and is for circulation within the organization.
- Internal Information/Data should be made available through Intranet/SVN/ E-mails to employees and to third party personnel with a business need to know.
- Softcopies of the document should be labeled as "Internal" and label should be in the centre of the header.
- 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 retention period.
  Media containing obsolete internal information/data should be destroyed/ formatted.
  Information asset owner should initiate the disposal.

10.3 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 the organization.
- Restricted Information/Data should be made available through Intranet/SVN/ E-mails to employees and to third party personnel with a business need to know.
- Softcopies of the document should be labeled as "Restricted" and label should be in the centre of the header.
- Hard copies of the "restricted" documents should be stamped in "Blue".
- 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 retention period.
  Media containing obsolete restricted information/data should be destroyed/ formatted.

Information asset owner should initiate the disposal.

10.4 Confidential

- 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 be provided.
- Softcopies of the document should be labeled as “Confidential” and label should be in the centre of the header.
- Hard copies of the “Confidential” documents should be stamped in “Red”.
- 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 the disposal.