GDC Network Access Security Conformance Agreement

I. User Password Usage

A. Systems Administrators' Responsibilities

1. Login name for user will be his / her LAN ID created as per GDC standards.
2. All accounts must have a password.
3. Default passwords for administrator and guest IDs will be changed.
4. Initial passwords assigned to users should not be easily guessed.
5. Users shall change their password on first logging.
6. Password change for every 120 days is mandatory.
7. Password information will be protected from general access. It will be kept in a closed and locked storage area within GDC.

B. Users Responsibilities

1. Users are not supposed to even accidentally type their password as the login name.
2. User name (first, middle or last) is not allowed to be part of password.
3. Users are not allowed to use near and dear names as password.
4. Users are not allowed to use common names or numbers such as house name, telephone numbers, driving license number, passport number etc.
5. Password should consist of at least one alphanumeric and one special character.
6. Users should use long passwords-minimum of 8 characters.
7. Users must not write down the password.
8. Users must not share their password with other users.

II. Personal Accountability

1. Force learning of other user passwords is not permitted. User is not allowed to crack or know another user password
2. Disrupting networking services are not allowed.
3. User will not share his/her account with other users
4. Tampering project-related data is not allowed.
5. Screen saver passwords are must and should be configured for 5 minutes idle time
6. Users are not allowed to take the data in any form outside the GDC area.
7. Project related data should be stored only on the designated area of server.
8. Users must not share their individual hard disk with other users.
9. Users will sign a "Secrecy Conformance Agreement" before being assigned a user account by the responsible systems administrator.
10. Users will not bring in or remove any form of magnetic media inside the GDC area. Also, he should not bring non-GDC user into the premises.
11. It is a violation to share your Access Control Card with anyone and is considered to be a breach of contract signed with Customer. Any such offense is punishable to the extent of termination.

III. Remote Access

1. Remote access in any form is not permitted to the GDC.
2. Equipment such as Remote Access Server (Hardware or Software) is not allowed inside the GDC.

IV. Disaster Recovery

A. For project related data

1. All project related data which needs to be backed up needs to be kept in the file server space provided, Centralized backup for project data. Daily, weekly and monthly backup for critical data to be defined along with retention period. Verification mechanism of weekly and monthly tapes should be in place as per GDC guidelines should be followed.
2. Use command specific tools for taking UNIX based backup.
3. Identify spare for critical components and keep the same either at GDC or off-site. If required, can have a SLA with vendors who are responsible for maintaining the hardware
4. GDC users shall not disable the antivirus software in their system and should ensure that updates are happening automatically.

V. Equipment Installation and Management

1. GDC employees are not allowed to bring and install any kind of hardware inside GDC area. Any electronic storage device such as PDA, USB stick etc. are strictly prohibited inside GDC area
2. Maintain complete hardware and software configuration records. As per the project plan for the project,
3. Keep a log of any client supplied hardware and associated spares.
4. Equipment allocated to the users should be protected with Due-diligence
5. Users shall connect only to those systems in the GDC / client network which are specifically mentioned in the project plan of the project the user is assigned to
6. GDC Systems Administrator will have complete control and verify installations of equipment and software configurations that provide access to the GDC Network to ensure that all appropriate security mechanisms are included in the

installations and that the installation adhere to GDC network addressing standards.

7. Any temporary installed hardware must not be connected to the network.

VI. Hardware and Software Licensing

1. Illegal use of duplicated software / programs / artifacts will NOT be permitted.
2. Unauthorized copies of licensed and copyrighted software will NOT be permitted to be used on GDC computer and network resources.
3. Users who have Internet access must not download shareware or freeware software. As per organization policy, only project permitted software are allowed. If any additional software needs to be installed, then prior permission from the GDC designated authority should be obtained.
4. If users have doubt about usage of particular software, they should immediately contact systems administrator for clarification
5. Unauthorized equipment configurations will not be permitted within the GDC and cannot be used to store or process Customer critical and/or sensitive data (user's private computer systems, modems, etc.)

These guidelines cover the employee when working in the RBC Global Development Center, India. When working at onsite, the local RBC network guidelines prevail.

I accept the RBC GDC Network Security Guidelines as a condition of employment with organization.

Employee Name: Sheik Nazarana

Emp. No:46237458

Employee Signature: sheiknazarana

Date: 05-07-2024

E-Mail ID: sheik.nazarana@capgemini.com

Secrecy Conformance Agreement

You have been assigned by the organization to perform contract services in the RBC Global Development Center (GDC). As a condition of your undertaking to perform contract service work for RBC it is necessary for you to agree to hold information which you learn about RBC during the course of this work in confidence, and further to provide that the results of your work will be owned by RBC. This Agreement is for the benefit of, and has been reviewed and approved by RBC

1. Conflict of Interest

You will not bring your personal interest of your previous employer in or out of GDC project. Also, you will warrant that refrain from any other activities, which would present a conflict of interest with your work on behalf of.

Should you leave the service of an employer, you are obliged to continue safeguarding the privacy of both clients and employees, and to protect the confidentiality of the company's business indefinitely. Specific client information -- including names, lists, profiles, data, etc. -- is not to be used in subsequent employment situations. Any client or proprietary information you have in your possession is to be returned to the organization when you leave.

2. Secrecy

You will warrant that you will not access, use, Disclose or remove any Restricted, Sensitive (ODC Internal information) form the ODC without the approval from the Delivery manager.

You will not disclose any information related to or associated group of companies, which you obtain or develop for . Also, you will agree that you will keep the proprietary, secret and confidential information within yourself, not disclosing to any other person or firm.

You are to avoid any conduct or association -- either inside or outside of work -- which could bring your honesty, integrity or trustworthiness into question, or which could be detrimental to security or to its reputation within the community.

3. Internet and Email

You are not to participate in any online forum, or send or display any material in a manner that can tarnish the image and reputation of the organization or

You will not to access or download games, songs, MP3, obscene or offensive material of any type

You will use organization corporate email ID only for business purpose.

4. Inventions

Any inventions, suggestions, ideas made by you as result of your services in GDC, shall to other be sole property of . You will assist

5. Copyrights

Any development material, copyrights of the same is reserved with . Publishing or use of these materials outside project interest, need prior approval from designated authority.

You are not to violate copyright, trademark or patent laws, or any other legal right of the organization or its Clients

6. Employer-employee Relationship

While rendering the services for GDC, you have to note that you will at all time be acting as an employee of . As such you will not be an employee of or your services performed are not entitled to participate in or receive any benefit under Employee Benefit and Welfare plans such as bonus, pensions etc.

7. Information Management Security Guidelines

You are required to follow organization policies, procedures and standards relating to Information Technology, Information Security and Privacy.

These security guidelines cover the following:

- Global Development Center (GDC) Security
- Desktop Security ♦ Network Security
- Password policy ♦ Security policy
- Acceptable usage policy

- Windows Operating System Security
- UNIX Security
- Application Security if any.

8. Security Alarm

Any observed or suspected Information Technology, Information Security or Privacy incidents or lapses are to be reported as expediently as possible to securityalarm@capgemini.com

9. Penalty

In violation of the above, you will meet with heavy penalty or subject to job termination and appropriate legal action.

If the above terms are acceptable to you as a condition for performing services for, please indicate your acceptance by signing one copy of this letter and returning it to us.

Employee Signature: sheiknazarana

Employee Name: Sheik Nazarana

Date: 05-07-2024

Employee ID: 46237458

Email ID: sheik.nazarana@capgemi

RBC SUPPLIER CODE OF CONDUCT

Purpose and Scope

This Supplier Code of Conduct ("Code") sets out our ("RBC") principles and expectations as to how organizations who supply goods and services to RBC ("Suppliers"), including their representatives and employees (together "Supplier's Employees") are to conduct business with and deal with us. We, Royal Bank of Canada and its subsidiaries, operate under the master brand name RBC.

In alignment with our values, we are committed to striking the right balance across shareholder groups, clients, employees and communities. Our values are built on providing excellent service to our clients and each other, a work ethic that promotes teamwork to succeed, taking personal responsibility for high performance, diversity for growth, and innovation and integrity in everything we do. Our organization, and all of our employees, have a duty to comply with applicable laws and regulations, and are expected to behave responsibly and ethically.

We expect Suppliers to operate in accordance with values comparable to ours and in a manner which is consistent with prudent business practices.

Business Integrity

Compliance with Laws

In all their activities, Suppliers must ensure they conduct business in compliance with the applicable laws, rules, and regulations of the jurisdictions in which they operate.

Conflicts of Interest

In their relationship with our employees, Suppliers must not try to gain improper advantage or preferential treatment for other relationships they may have with us (for example, as a client).

Gifts and Entertainment

The nature of the gifts or entertainment must not, by their quality, quantity or timing, be used by Suppliers to gain improper advantage or preferential treatment. We expect that Suppliers will maintain appropriate records of exchanges of gifts and entertainment with our employees.

Anti-bribery and Anti-Corruption

Suppliers must not engage in any conduct that would put our organization at risk of violating anti-bribery laws.

Inside Information and Information Barriers

In their dealings with us, if Suppliers become aware of inside information about us or our clients, we expect Suppliers to have in place policies and procedures for the proper handling and use of that information (such as information barriers). These policies and procedures must meet applicable legal and regulatory requirements to prevent inappropriate access or disclosure of inside information.

Responsible Business Practices

Privacy and Information Security

Suppliers must comply with RBC's published Privacy Policy, and must use information obtained through their relationship with us only for the purpose defined to them.

Suppliers must store information as agreed with RBC and have appropriate information security policies and procedures in place to secure access to our information. Suppliers must notify us promptly of actual or suspected privacy breaches, security breaches, or losses of our information.

Business Resumption and Contingency Planning

For some services performed by Suppliers, due to the significance for our businesses or the types of activities that may be involved, we expect that the Supplier's business continuity and disaster recovery plans are developed, maintained and tested in accordance with applicable regulatory, contractual and service level requirements.

Outsourcing and Subcontracting

We recognize that outsourcing is a practice that Suppliers may use to promote innovation, fill resource gaps, and/or create operational efficiencies. We also recognize that Suppliers may need to use subcontractors in the performance of services. However, we expect Suppliers not to subcontract services they perform for us or outsource activities that directly impact the delivery of goods and services to us, without our prior written approval. In situations where approval is given, it is important for us to know the locations of where the work will be performed and the parties involved in the provision of the services.

In addition, Suppliers must monitor the outsourcing or subcontracting arrangement to ensure it complies with the Suppliers' contractual obligations and with this Code, and provide evidence of such monitoring upon request.

Responsible Treatment of Individuals

Respect and Diversity

Suppliers must maintain workplaces characterized by professionalism, and respect for the dignity of every individual with whom their employees interact. Suppliers must respect the diversity of their employees, clients and others with whom they interact, including respect for differences such as gender, race, colour, age, disability, sexual orientation, ethnic origin and religion. Suppliers must not tolerate harassment, discrimination, violence, retaliation and other disrespectful and inappropriate behaviour.

Suppliers must respect the dignity of their own employees and others, adhere to principles of diversity and maintain a respectful workplace. See the link to our Code of Conduct under Governance Information.

Employment Practices

Suppliers must abide by applicable employment standards, labour, non-discrimination and human rights legislation. Where laws do not prohibit discrimination, or where they allow for differential treatment, we expect Suppliers to be committed to non-discrimination principles and not to operate in a way that differentiates unfairly.

Suppliers must be able to demonstrate that, in their workplaces:

- Child labour is not used.
- Discrimination and harassment are prohibited, including discrimination or harassment based on any characteristic protected by law.
- Employees are free to raise concerns and speak up without fear of reprisal.
- Appropriate and reasonable background screenings, including investigations for prior criminal activity, have been done to ensure the integrity and good character of the Supplier's Employees.
- Clear and uniformly applied employment standards are used that meet or exceed legal and regulatory requirements.

Health and Safety

We expect Suppliers to provide healthy and safe workplaces and comply with relevant health and safety laws. We expect Suppliers to provide all their employees with adequate information and instruction on health and safety concerns and to enable their employees to meet their responsibilities for the maintenance of a healthy and safe workplace.

Environment

We expect Suppliers to work with us to promote environmental sustainability. Suppliers are to assist in reducing our environmental footprint, conduct business in an environmentally responsible way, and offer environmentally responsible products and services. See our public policy - RBC Environmental Blueprint

Record keeping

Suppliers must not destroy our records that may be relevant to any pending or threatened legal or regulatory proceeding of which the Supplier becomes aware. Suppliers must maintain adequate internal records to ensure proper compliance with their obligations to us.

Code Compliance and Monitoring

We expect Suppliers to comply with this Code. For some services, because of their significance for our business and the type of activities they involve, we may require a Supplier to periodically confirm in writing to our Chief Procurement Officer, that they meet the requirements of this Code. In addition, we must be able to monitor and audit a Supplier's control environment.

Failure to comply with this Code may result in termination of a Supplier's relationship with us.

Appendix on Canadian Content

RBC is committed to a continued focus on Canadian jobs and prosperity in our Supplier arrangements and policies, balancing our desire to be both a successful business and a leading corporate citizen. Our business decisions are based on striking the right balance across all stakeholder groups – clients, employees, shareholders, and communities and in alignment with our values. As RBC enters into Supplier relationships, a key component of that decision is to ensure our Suppliers share and hold similar values and principles across their organizations.

In addition to complying with the Supplier Code of Conduct, RBC expects that Suppliers that provide services to RBC in Canada, which will support our commitment to focus on Canadian jobs and prosperity and meet these more specific standards. Failure to comply may result in termination of a Supplier's relationship with RBC.

1. Suppliers will not make any application, written or otherwise to any government body on behalf of RBC without RBC approval.
2. Suppliers will not hire foreign workers from outside of Canada when performing services on behalf of RBC, where a worker eligible to work in Canada is available and able to perform the service.
3. Suppliers will notify RBC immediately if they have been in breach of any Canadian Human Rights, employment standards (legal and regulatory) or immigration laws.
4. Suppliers will not implement any material change to the way services are provided to RBC that has an impact on the Suppliers' employees, without consulting RBC to ensure there is no breach of our policies and the Supplier Code of Conduct.
5. Suppliers will not sub-contract services without the specific written consent of RBC. To obtain consent Suppliers will be required to make available/disclose to RBC the specific contractual arrangement with the sub-contracted party.
6. Suppliers, by their action and in collaboration with RBC need to demonstrate that they continue to create investment and jobs in Canada in the provision of service to RBC.

To support our joint commitment to Canada, Suppliers may be asked to provide regular written confirmation to RBC's Chief Procurement Officer of their compliance to the Supplier Code of Conduct and this appendix.

Employee Name: Sheik Nazarana

Employee ID: sheik.nazarana@capgemini.com

Privacy Notice: Important Notice Concerning Your Privacy: Please Read this Carefully

Please be notified that RBC is enabling **Data Loss Protection** monitoring and investigation processes – which will include monitoring of all email/electronic communications. All employee communications using the RBC email accounts shall be part of the Data Loss Protection monitoring and will inevitably include all employee non-business communications using RBC email accounts.

Use of RBC email accounts for non-business communications shall be construed as consent by the employee to such monitoring.

Capgemini Data Privacy Policy notifies all employees of the monitoring of the use of the company's network resources, such as emails, internet, etc. Please read this Policy carefully.

Please acknowledge receipt of this Privacy Notice

Signature: sheiknazarana

Name: Sheik Nazarana

Employee ID: 46237458