BCE Global Tech Security Policy

Commitment to Security

At BCE Global Tech, we prioritize the security of our users' data and our digital infrastructure. We implement robust security measures to protect against unauthorized access, data breaches, and other security threats.

Security Measures

Data Encryption: All sensitive data is encrypted in transit and at rest.

Access Control: Strict access controls are in place to ensure that only authorized personnel can access sensitive information.

Regular Audits: Conducting regular security audits and vulnerability assessments to identify and mitigate potential risks.

User Responsibilities

Users are expected to follow best practices for security, including using strong passwords and not sharing login credentials.

Incident Response

In the event of a security incident, we have a comprehensive incident response plan to quickly address and mitigate the impact.

Contact Information

For security-related inquiries or to report a security issue, please contact us at info@bceglobaltech.com.

BCE Global Technology Centre Private Limited (BCE GTC), a subsidiary **of Bell Canada Enterprises**, is dedicated to delivering innovative telecommunications solutions while ensuring the highest standards of information security. As a leading provider in the telecom industry, we recognize the critical importance of safeguarding our information assets and maintaining the trust of our customers, partners, and stakeholders.

Commitment to Information Security

At BCE GTC, we are committed to implementing and maintaining a robust Information Security Management System (ISMS) that aligns with international standards such as ISO 27001, NIST and Information Security Forum (ISF) frameworks. Our commitment to information security is driven by the following principles:

Confidentiality: Ensuring that information is accessible only to those authorized to have access.

Integrity: Safeguarding the accuracy and completeness of information and processing methods.

Availability: Ensuring that authorized users have access to information and associated assets when required.

Strategic Objectives

Our security controls are organized under ten strategic pillars and applied to nine asset classes to ensure comprehensive protection across our organization. These controls include but are not limited to:

The 10 Strategic Information Security pillars are:

1. **Asset management & visibility:** Complete discovery and management of all relevant BCE GTC assets, federated into a single view.

2. **Access control and authentication:** Centralize and govern all aspects of digital identity and enhance customer authentication.

3. **Secure system development & operations**: Develop, support, and patch systems in compliance with secure practices and ensure business continuity.

4. **Application, network, and endpoint security:** Establish multiple layers of defence across network, endpoint, database and storage to enhance protection.

5. **Security testing:** Prioritize and conduct testing for vulnerabilities and intrusion risks

6. **Policies, requirements & risk prioritization:** Define requirements, develop policies and ensure effective risk identification and prioritization.

7. **Supplier Risk Management:** Assess supplier access to infrastructure and data and ensure adequate controls are in place.

8. **Security skills, education and awareness:** Drive a cultural shift on Information Security sensitivity across BCE GTC and ensure adequate skills.

9. **Cyber Threat Intelligence and detection:** Monitor, detect and proactively take action on current and emerging threats.

10. **Incident response & recovery:** Ensure efficient and diligent coordination of Information Security incident response across BCE GTC.

The 9 asset classes encompass the entire IS/IT and network asset fleet across BCE GTC:

1. **Websites:** All assets delivering browser-based internet services containing a URL including internal hosted, public hosted and hybrid types.

2. **Corporate Applications:** Corporate applications include some form of business logic used by team members, partners and/or contractors, regardless of whether the application is developed internally or externally, or where the application is physically hosted. This includes, application program interfaces (API), software as a service application (SaaS), DNS, Active Directory, and corporate VPN solutions.

3. **Customer Applications:** BCE GTC customer applications are where the customer has an interface into the application, regardless of where the application is hosted internal or external hosted, developed in house or externally, running on BCE GTC infrastructure, or on a customer asset.

4. **Databases:** Database systems that are either standalone, supporting applications or websites. Typically, this category includes Oracle and MS-SQL. This category excludes Big data and Data mart systems such as: Hadoop, Hortonworks.

5. **Servers/Mainframe/Software:** This category includes all server platforms both chassis based and virtual, including MS-windows and Red Hat Linux. This category also includes the mainframe and midrange servers including ZOS, AS/400. All server software, excluding the previously defined application and database categories is also included here. This would include all system management and maintenance software on the servers including backup software, asset management software, middleware software, access management software and security software.

6. **Network Elements:** Any physical/virtual/appliance device, or software, that supports the transmission of data, including protocol conversion, load balancing, packet analysis and packet filtering where the operating system and service(s) are managed and maintained as one entity and optimized for specialized purpose.

7. **Endpoints/Mobile Devices:** This includes any user device such as desktop, laptop, tablet, mobile device or printer. Internet of things (IoT) devices are also included in this asset category.

8. **Messaging & Collaboration:** This includes messaging and collaboration systems, such as email, instant messaging, collaboration, file sharing, and video conferencing.

9. **Big Data Lakes & Warehouses:** All instances of Data Lakes, & Warehouses supporting business intelligence. Data can be of any type, structure or source. These environments are typically large-scale data storage for analytical queries or machine learning and are central repositories of integrated data from one or more disparate sources.

Responsibility and Accountability

Information security is the responsibility of every employee at BCE GTC. Our leadership team is committed to providing the necessary resources and support to implement and maintain our ISMS. All employees are expected to adhere to our information security policies and report any potential security breaches or weaknesses.

Contact Information

For security-related inquiries or to report a security issue, please contact us at info@bceglobaltech.com.