BICS Corporate Security Statement

Belgacom International Carrier Services (BICS) takes the security of its information, infrastructure and applications very seriously. Its commitment to corporate security is shown through the implementation of policies, controls and procedures, as well as the allocation of dedicated resources required for a formal Corporate Security organization.
This document provides an overview of the security controls employed by BICS and is intended to be shared with its current and potential customers and suppliers.

Security Policy

BICS provides its employees with security policies and guidelines to communicate individual responsibilities with respect to safeguarding BICS' resources. These policies are readily available to employees through the intranet portal. BICS security framework in place is built following ISO/IEC 27001:2022. All BICS new hires are required to undertake a series of training sessions, which among other issues address partner and staff responsibilities as they relate to our Code of Conduct, local policies and procedures, Information Security, and privacy. BICS partners and staff are required to complete an individual confirmation of their responsibility for the security of BICS' information to which they are granted access and to take due care to protect the technology equipment assigned to them.

Security Organization

Internal Security Organization

BICS has a formal Corporate Security organization led by the Chief Information Security Officer (CISO), who is responsible for all the security matters in the Organization and is assisted by a team of technology and security professionals. The CISO reports to a Corporate Security & Business Continuity & Privacy Committee and has the ultimate responsibility for the Organizations security-related decisions and strategies. These security professionals hold a variety of certifications and other credentials that attest their proficiency in the field. They participate in training programs and activities sponsored by industry-specific security groups to stay abreast of current security trends and issues.

Confidential Agreements

All BICS' employees (incl. contractors), upon joining the Organization and/or during their employment period, as well as certain service providers, are required to sign non-disclosure and confidentiality agreements, demonstrating their commitment to the Organization and its information security.

Asset Management

Asset Inventory and Classification

BICS has established and maintains asset inventory processes for its main physical and information assets. BICS' information security policy defines a four-tier scheme for classifying its main information assets, which are:

- Determination of the data classification level of information assets
- Identification of the information owner
- Identification of security risk factors
- Identification of disaster recovery risk factors

Information Handling

Information subject to legislative or regulatory requirements is identified through the asset inventory process. Security controls are established to address the relevant requirements. BICS professionals are regularly provided with instructions on identifying and handling the Organization's information.

Human Resources Security

People connecting to the BICS network are required to conduct themselves in a manner consistent with the Organization’s security policies regarding, among other matters, confidentiality, business ethics and professional standards. BICS requires that communications via these connections comply with applicable laws and regulations, including those governing:

- Restrictions on the use of telecommunications technology and encryption
- Copyrights and license agreement terms and conditions

Confirmation of Security Responsibilities

All BICS staff (employees and contractors) must participate in the Organizations annual regulatory process for Compliance Confirmation. This process requires that the BICS staff provide an individual confirmation of their responsibility for the security of BICS’ information to which they have access, and to take due care to protect the technology equipment assigned to them. All staff members sign a personal liability agreement acknowledging their responsibility for the professional equipment and tools received to develop their work, being also responsible for the physical security of these assets.

Appropriate use

The BICS Code of Conduct and the Information Security Policy address the appropriate use of electronic tools and technologies. Those who violate the Code or BICS policies and procedures will be subject to the sanctions established by the labor legislation in force, up to and including dismissal, depending on the seriousness of the violation.

Security Awareness Training

Security awareness training is a component of the BICS hiring process. An awareness program reinforces periodically the concepts and responsibilities defined in the Information Security Policy.

Termination Processes

BICS has established documented termination processes that define responsibilities for collection of information assets and removal of access rights for professionals who leave the Organization.

Physical and Environmental Security

Data Center Security

The following physical and environmental controls are incorporated into the design of the BICS Data Center:

- Separate protected facilities
- Badge entrance control
- Internal and external cameras
- Temperature and humidity control and monitoring
- Smoke detection alarm
- Lightning suppression
- Transient voltage surge suppression and grounding
- Redundant power feeds and UPS Systems
- Physically secured network equipment areas and locked cabinets

Data center access is limited to authorized personnel. Visitor access procedures and loading dock security protocols are established.

BICS' Office Security

Physical access controls are implemented at all BICS offices. Controls vary by location but typically include card-reader access to facilities, on-premises security staff and defined procedures for visitor access control.

Communications and Operations Management

Operational Procedures and Responsibilities

BICS' IT organization has established and maintains controls over standard operating procedures, including a repository of procedures, formal review and approval processes, and revision management.

Change Control

BICS' IT organization has established and maintains a Change Management/Change Control process which includes risk assessment, test and retrieval procedures and review and approval components.

Development Environments

BICS maintains separate development and production environments. Development environments are required to be physically separated from production environments. The transfer of an application from development to production follows the procedures established in the Change Management/Change Control process.

Wireless Networks

Only IT-managed wireless networks are permitted on BICS' network. The wireless network is segmented to ensure only fully managed endpoints are admitted to the corporate network while unmanaged endpoints, are placed on a guest Vlan, and at best with access to internet. Wireless access security controls include standards for encryption and authentication that are managed by Proximus.

System Backup

Data center systems are routinely backed up for disaster recovery purposes. Restoration success metrics are maintained. BICS utilizes an information protection and storage provider for secure transport and offsite storage of backup media.

Security Software Suite

BICS uses a combination of technology tools to provide a secure computing environment equipped with:

Antivirus

the virus protection software package is loaded during the operating system start up process and performs on-access scans of all data. The software is configured to clean or delete infected files and provides other safeguards. Virus signatures are automatically and constantly updated through a process managed on a central basis.

Antispyware

BICS installs spyware detection and removal of malicious software on all the Organizations computers.

Desktop Firewall

BICS' desktop firewall software is automatically enabled and uses the Organizations standard configuration to protect against malicious network traffic, including internet-based network threats, untrusted networks or malicious software. Database configuration settings are secured against change, tampering or disablement by end users or malicious programs.

Secure Remote Access

BICS utilizes virtual private network (VPN) software, configured to require dual factor authentication to enable secure remote access to its networks.

Microsoft Office

BICS uses Microsoft Office for a number of applications, including e-mail. Microsoft Office' security features are widely recognized in the market.

Full disk Hard Drive encryption

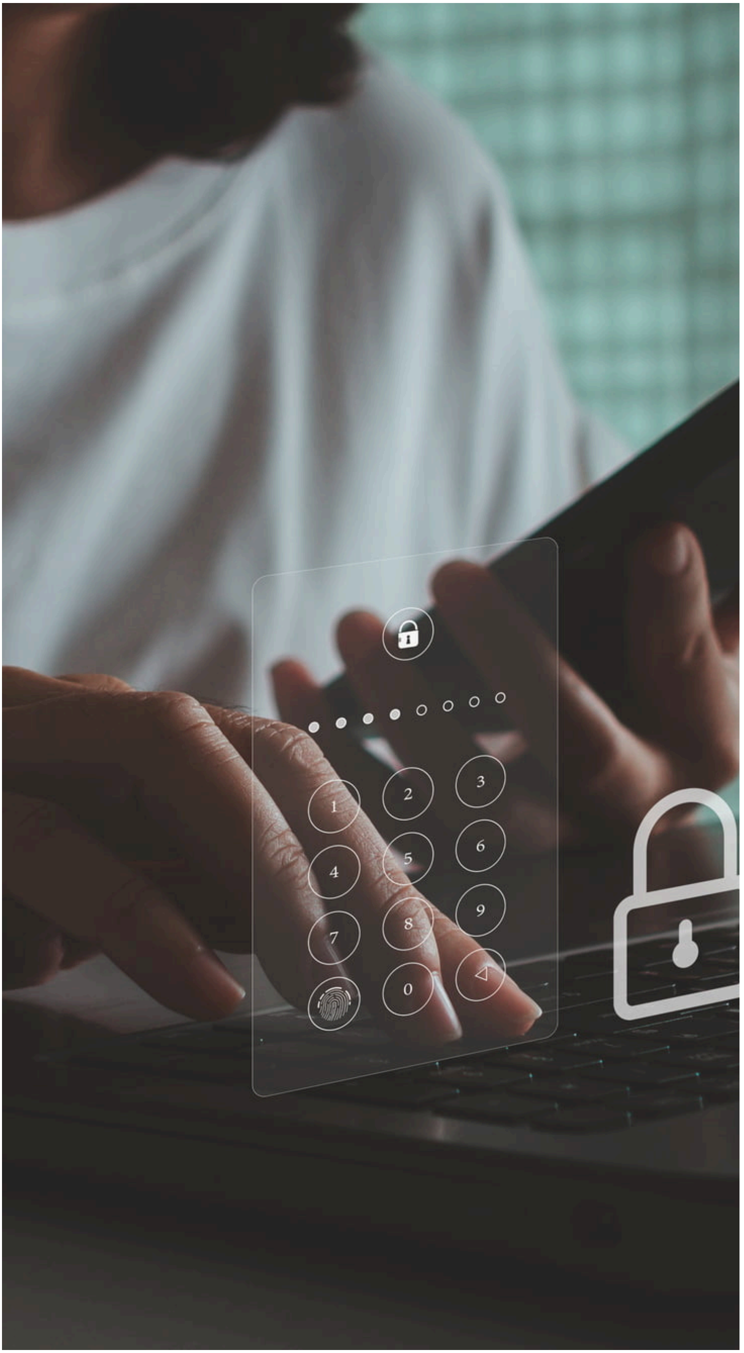
is being used in order to prevent most offline physical attacks and boot sector malware.

SIEM (security information and event management)

is being used for security monitoring and anomalies detection.

Spam Blocking and URL Filtering

BICS has deployed and regularly updates URL filtering software that blocks access to inappropriate web sites from its network. BICS has also established and maintains e-mail gateway with spam-blocking and anti-virus software (fully controlled by Proximus).



Access Control

Authorization and Authentication Controls

BICS follows a formal process to grant or revoke access to its resources. System access is based on the concepts of "least-possible-privilege" and "need-to-know" to ensure that authorized access is consistent with defined responsibilities. The Organization uses a combination of user-based, role-based and rule-based access control approaches. BICS has established documented procedures for secure creation and deletion of user accounts, including processes to disable and/or delete accounts of employees temporarily away from the Organization. All BICS staff are required to agree to take reasonable precautions to protect the integrity and confidentiality of security credentials.

Privileged Access

Access to authentication servers at administrative, root or system levels is limited to those professionals designated by BICS.

Password Requirements

The Organizations security policy establishes requirements for password changes, reuse and complexity. BICS requires the use of session lock after a period of inactivity through the use of a password.

Remote Access

BICS uses virtual private network (VPN) software to enable secure, internet-based remote access for its professionals. VPN users are required to authenticate using two-factor authentication; both a valid user name/ password and a corresponding password-protected VPN token are required to create a VPN tunnel.

VPN tunnels are secured using AES128 or higher encryption. The client software uses smart tunneling technology to ensure that communications between the host PC and the BICS network are transmitted via an encrypted

VPN tunnel. Communications to internet-routed addresses will be conducted outside of the established VPN tunnel. Also, session timeout settings are configured to automatically disconnect the user from a session after a period of mouse or keyboard inactivity. Processes are established to limit third-party remote access to BICS systems. Such access requires approval from the security team and access is limited to those systems required for the third-party to complete the task and is monitored on a regular basis.

Computer Security

All BICS desktops and laptops are protected by hard drive encryption software through the 256-bit AES encryption algorithm. The software enforces password controls and uses a dynamic password time-out to prevent brute force password attacks. Additionally, the software is bound to the hard drive, protecting not only the operating system, but also the data. The internal policy that regulates the use of laptop is widely disclosed to BICS staff. Training is delivered to new employees to educate them about theft and to encourage behavior that will help protect laptops against it.

Mobile Devices

Mobile device access is only permitted in accordance with the Organizations security policy and requires a password to be entered to access the device. The information on the device will be erased after ten incorrect access attempts and remote erasure is made if the device is reported lost or stolen.

Information Systems Development Cycle

BICS has established a methodology to manage the acquisition, development and maintenance of systems. Key security components related to this methodology include:

- Business criticality assessment
- Risk assessment
- Security team involvement in project reviews and key contracts
- Utilization of established change control processes to transfer changes from the development to the production environment
- Penetration testing of a new service/ significant change

Internal and External Network Scanning

BICS utilizes multiple vulnerability scanning tools to assess its internal and externally facing network environments. These tools are selected and configured to match the requirements of BICS' IT infrastructure, and are updated on an ongoing basis. Processes are established to assess and correct the vulnerabilities discovered.

Patch Management

BICS has patch management processes and tools to assess and deploy operating system and application-specific patches and updates. This process includes steps to evaluate vendor supplied patches to determine servers that require patches and updates, to document procedures for patching and updating servers, and to deploy patches and updates in a timely manner to protect the BICS infrastructure. BICS continually reviews patches and updates, as they are released, to determine their criticalities. Patches released on a regularly scheduled basis are applied following the release; patches released on a regular basis and others determined to be critical are applied as needed to ensure protection from vulnerabilities.

Information Security Incident Management

BICS staff members are made aware that security incidents must be reported immediately. BICS has documented procedures for the receipt of security incident reports. BICS Corporate Security team has a documented incident response process which includes:

- Escalation process
- Pre-defined roles and responsibilities
- Incident response plan

Business Continuity and Disaster Recovery Management

BICS has established a Business Continuity and Disaster Recovery process, following the guidelines of the Business Continuity Institute. To manage this process properly BICS has appointed a Business Continuity Manager and a deputy Business Continuity Manager. BICS has a BCP strategy approved by its executive management; this strategy is documented and shared on the internal BICS network.

Within the BCP strategy it is defined for which products and services (including ICT infrastructure) BICS develops a BCP and DRP plan. These plans are regularly reviewed, updated and tested. Apart from the BCP and DRP documents for the services/products BICS has also a Denial of Access Procedure; this will allow BICS to continue working in emergency instances.

Compliance

Vulnerability Scanning

BICS has established processes for performing periodic vulnerability scans of its IT systems. These procedures specify the use of multiple vulnerability scanning software packages, the creation of vulnerability assessment reports, and the presentation of vulnerability scanning results to the IT Operations organization and IT leadership. Access to vulnerability scanning tools is restricted to authorized members of the security team.

Internal Audit

BICS has an Internal Audit organization responsible for assessing internal operations, including the Security and IT teams.

Ethics & Compliance

BICS has implemented procedures to report, either anonymously or not, any misconduct of its professionals or third-parties with respect to the Code and laws and regulations referring to property, secrecy, confidentiality, ethics, business conduct, as well as to internal policies and procedures.

Privacy Office

BICS has established Data Protection rules that define, among other issues, the standards of behavior regarding the protection of BICS information.

Date : July 2023
Owner : BICS Corporate Security team
Classification : Unrestricted
Next review planned in July 2024

Disclaimer

In this document, “Belgacom International Carrier Services“ (“BICS” or “Organization”) refers to BICS SA/NV., which is a member of Proximus, and its Affiliates.

The intent of this statement is to provide a brief overview of the security measures implemented to help protect the BICS information, infrastructure and applications. It does not represent all efforts made by BICS to mitigate the risks related to Information Technology.

These security measures do not guarantee complete protection. The information contained in this statement is for current or potential customers and suppliers and should not be distributed to others without permission from BICS.

For more information

www.bics.com/security