

IT SECURITY POLICY

BRIGHTSTAR N.V.
Kaya W.F.G., (Jombi) Mensing 24,
Unit A
Willemstad | Curaçao

Last Updated 23.12.2024

PURPOSE

This IT Security Policy establishes the procedures and standards required to ensure that all Windows and MacOS devices owned or managed by Brightstar N.V. are safeguarded through regular updates of security patches, operating system updates, and antivirus definitions. By maintaining a proactive approach to device security, the policy aims to protect sensitive data and uphold the integrity, availability, and confidentiality of the organization's digital assets, mitigating vulnerabilities that could lead to security breaches.

SCOPE

This policy applies to all organization-owned or managed Windows and MacOS devices, as well as the Bitdefender antivirus software installed on these systems. It encompasses all employees, contractors, and third parties utilizing organizational devices for any operational purposes.

POLICY STATEMENTS

1. Automatic Updates and Security Patches

- Windows OS:

All Windows devices must have automatic updates enabled to ensure timely receipt of critical security updates and patches. These devices are required to check for updates daily, with installations scheduled during non-working hours to minimize operational disruption.

- MacOS:

All MacOS devices must also have automatic updates enabled. The IT department is responsible for verifying that updates, particularly security patches, are applied promptly upon release. Devices will check for updates daily, with installations scheduled during off-peak hours to prevent interference with business operations.

- Bitdefender Antivirus:

All devices equipped with Bitdefender antivirus must have automatic updates enabled to maintain real-time protection. Updates for virus definitions and related software must be applied multiple times daily to counter emerging threats effectively.

2. Security Update Management

- Routine Checks:

The IT department will conduct weekly compliance checks to ensure that all organizational devices are updated with the latest security patches. Any non-compliant devices will be flagged for immediate intervention to address vulnerabilities.

- Security Patch Testing:

Critical security patches must be tested in a controlled environment prior to organization-wide deployment. This ensures compatibility with essential business applications and minimizes the risk of disruptions to operations.

3. Vulnerability Management

- Regular Vulnerability Scans:

Bi-weekly vulnerability scans will be conducted on all Windows and MacOS devices to identify potential security risks. Any vulnerabilities detected will be assessed based on severity, and necessary patches or mitigation steps will be prioritized.

- Third-Party Software Updates:

All third-party applications, including but not limited to web browsers, PDF readers, and productivity tools, must be regularly updated to address known vulnerabilities. The IT department will monitor and enforce compliance.

4. Bitdefender Antivirus Policy

- Automatic Virus Definition Updates:

Bitdefender antivirus is configured for automatic virus definition updates to ensure that all devices are equipped with the latest protection against evolving threats. Updates will run multiple times daily to capture new risks promptly.

- Scheduled Scans:

Bitdefender will perform a weekly full-system scan on all devices, in addition to daily scans of critical system areas. The IT department will review scan reports and address any detected threats to prevent further issues.

- Threat Response:

In the event of a detected threat, Bitdefender will immediately quarantine and log the incident. The IT department will investigate the threat and implement corrective measures to mitigate future occurrences.

5. Secure Payment and Data Protection

Player credit card numbers stored on the Applicant's system are protected in accordance with the Payment Card Industry Data Security Standard (PCI DSS). This includes encryption of data at rest and in transit, restricted access controls, and regular security assessments.

6. Security Administration Activities

Brightstar N.V. enforces strict access control measures to safeguard sensitive information and systems. Access to applications, data, and operating systems is granted on a need-to-know basis, aligned with defined job roles and responsibilities. A role-based access control (RBAC) system is used to manage user permissions and ensure that access rights are commensurate with management's control objectives. All access attempts are logged and monitored for any unauthorized activity.

ROLES AND RESPONSIBILITIES

1. IT Department:

- Enforce the IT Security Policy across all organizational devices.
- Manage and configure automatic updates for operating systems and antivirus software.
- Monitor compliance and conduct regular vulnerability scans.
- Test and deploy critical updates to ensure compatibility and system stability.

System User Access Control

All system users must have their identities verified before being granted access to the Applicant's systems. Identity verification is achieved through a unique account identifier

and a strong password combination, or a method offering equal or greater security. These measures ensure that access to sensitive data and systems is restricted to authorized personnel only. Access rights are assigned based on job responsibilities and the organization's security objectives, adhering to the principle of least privilege. All access attempts are logged and monitored for any unauthorized activity.

2. Device Users:

- Avoid disabling or interfering with automatic updates, security patches, or antivirus functions.
- Report any issues or anomalies related to device security to the IT department immediately.

3. Player Account Security

All players must have their identity verified before accessing the system. This is achieved through a unique account identifier and a strong password combination. To further enhance security, email verification is also implemented.

MONITORING AND COMPLIANCE

Compliance with this policy will be monitored through periodic reporting and audits. Devices found to be non-compliant with automatic updates, security patching, or antivirus policies will be subject to corrective action. This may include notifying users, conducting mandatory updates, or temporarily suspending device access until compliance is restored.

Transaction Monitoring and Audit Logs

All deposit, withdrawal, and adjustment transactions are subject to rigorous security controls, including fraud detection mechanisms and multi-factor authentication. A comprehensive system audit log records all transaction details, including user IDs, timestamps, and transaction amounts. The audit log is securely maintained and regularly reviewed for any suspicious activity.

EXCEPTIONS

Any exceptions to this policy must be formally documented, justified through a risk assessment, and approved by the IT Security Manager. Exceptions will be reviewed periodically to ensure they remain valid and do not compromise overall security.

POLICY REVIEW AND UPDATES

This IT Security Policy, guided by a risk-based approach, will be reviewed annually alongside relevant risk assessments to address advancements in technology, changes in regulatory requirements, and evolving organizational needs. Risk-based internal and external security reviews will be conducted at least annually, or more frequently in response to material changes. Updates will be communicated to all relevant stakeholders to ensure ongoing compliance and awareness.