

Information Security Procedure

Ex Lux N.V.

Document Control

Version	Date	Description of Changes	Author
1.0	04.03.2026	Initial draft	IGA Trust B.V.

1. POLICY

To protect all company information—from written or printed materials to electronic data—from unauthorized access, modification, destruction, or disclosure throughout its lifecycle.

2. Key Points

Documentation: All policies, procedures, and related activities must be documented and accessible to responsible staff.

Retention: Documentation must be kept for at least 5 years from creation or modification and reviewed regularly for accuracy and relevance.

Departmental Policies: Departments may develop additional policies and procedures, which must align with this overall policy.

System Compliance: New systems must comply with this policy. Existing systems should be updated to comply as soon as practical.

3. RISK MANAGEMENT

Risk Identification: All departments must identify threats and vulnerabilities affecting information assets, systems, and processes.

Risk Assessment: Evaluate risks by their likelihood and potential impact on information security and business operations.

Risk Treatment: Implement controls to mitigate, transfer, accept, or avoid risks, prioritizing high-impact risks.

4. INFORMATION SECURITY RESPONSIBILITIES

4.1 The Information Security Officer (ISO) is responsible for developing, implementing, and enforcing security policies and controls, supporting users and systems, advising on classification and secure system design, providing ongoing training, and conducting regular security audits within each entity, subject to approval by EX LUX N.V.

4.2 The Information Owner is responsible for understanding, protecting, and managing their information, including determining retention, authorizing access, assigning custodians, specifying controls, reporting incidents, initiating corrective actions, promoting awareness, and following approval processes, with delegation permitted when authorized.

4.3 The Information Custodian is responsible for securely processing, storing, and administering information according to owner-specified controls, implementing safeguards, managing access,

supporting awareness and policies, evaluating controls, reporting incidents, and responding to security issues in consultation with the ISO.

4.4 User Management is responsible for overseeing employee use of information by approving access, updating security records, managing terminations and transfers, providing training, reporting incidents, initiating corrective actions, and following organizational approval processes for systems and software.

4.5 A User is any authorized individual who must access information only for their job, comply with security policies and controls, keep authentication credentials confidential, report incidents to the ISO, and take corrective action when issues arise.

5. INFORMATION CLASSIFICATION

5.1 Information classification ensures appropriate controls to protect confidentiality, while integrity and accuracy must be maintained for all information. Classification depends on sensitivity and applies consistently across all formats.

5.2 Highly sensitive information restricted to those with a legitimate business need. Examples: personnel data, key financials, passwords, encryption keys. Unauthorized disclosure may violate laws or harm EX LUX N.V., its customers, or partners. Access must be approved by the information owner.

5.3 Intended for use within EX LUX N.V. or affiliated partners. Examples: internal directories, policies, most internal emails. Any information not classified as Confidential or Public defaults to Internal. Unauthorized external disclosure may be inappropriate.

5.4 Approved for release outside the company. Examples: marketing materials, website content. This information may be freely shared externally.

6. COMPUTER AND INFORMATION CONTROL

6.1 All systems and information are assets of EX LUX N.V. and must be protected from misuse, unauthorized access, and destruction through physical and software safeguards.

6.2 All software developed or licensed for EX LUX N.V. is company property and must comply with licensing agreements and acquisition policies.

6.3 Approved virus protection must be deployed across all systems; users may not disable these protections.

6.4 Access to Confidential and Internal information is restricted based on need-to-know, roles, or user identity, with authorization by supervisors and the ISO. Users must have unique

authentication (passwords, biometrics, or tokens), secure credentials, and log off when not in use. Physical access to systems and workstations must be controlled; emergency access procedures must be documented.

6.5 Ensure data integrity through audit logs, RAID, encryption, checksums, and digital signatures. Transmitted data must have appropriate encryption and integrity controls. Remote access must use approved devices and maintain the same protections as on-site systems.

6.6 Information disposal and media reuse must protect Confidential and Internal data (e.g., degaussing, shredding, or destruction of storage devices). Mobile and external media must be secured and encrypted; breaches make the owner accountable.

6.7 Mass data transfers and printing of Confidential/Internal information require authorization and minimization of data. Information used for research should be de-identified whenever possible.

6.8 Confidential information should not be discussed in public or semi-public areas where it can be overheard.

6.9 Audit logs and activity records must be maintained and regularly reviewed; periodic evaluations are required to ensure ongoing protection.

6.10 Each entity must maintain plans to recover from emergencies or disasters affecting systems or information, ensuring restoration of Confidential and Internal data.

6.11 EX LUX N.V. must maintain a documented and regularly tested backup and contingency plan that ensures secure, retrievable copies of all critical data, supports disaster recovery and emergency operations, and includes an assessment of application and data criticality.

7. COMPLIANCE

7.1 Curaçao Replication Server (Mandatory for Player Data):

- Ex Lux N.V. must perform regular backups of **player data** to a centralized server located in Curaçao, managed by an approved third-party provider.
- The backup must include all critical information and be maintained in a secure, retrievable format.
- CGA must have access to the Curaçao backup to ensure oversight and compliance.
- The provider is responsible for ensuring that all backups meet the same security and integrity standards as local backups
- EX LUX N.V. retains ultimate accountability for the integrity and availability of all player data, even when managed by the third-party provider.

