

Version	Date	Security Class	Responsible Person	Purpose
V1.0	27th June 2025	Confidential	Chief Technical Officer	Creation of this document

INFORMATION SECURITY POLICY

Purpose

BALKAN INTERNATIONAL N.V. must protect the confidentiality, integrity and availability of all of its business information to safeguard the company's assets, stakeholders and reputation, irrespective of its form (electronic, on paper, spoken and etc.). Information must be available only to those authorized to access it and there must never be any doubt that the information is complete and correct. This policy forms part of **BALKAN INTERNATIONAL N.V.** Corporate Governance.

Policy Basis

This information security policy has been based on a number of documents, but the main sources are:

- ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management).
- Payment card Industry (PCI) Data Security Standard V1.2 (October 2008).
- Securities Exchange Commission: Sarbanes-Oxley Sections 302 & 304.

Responsibilities

The teams/person responsible for the implementation and effectiveness of this policy are:

- Executive Board
- ISO (Information Security Officer)

Policy Objectives

The objectives of this policy are:

- To protect **BALKAN INTERNATIONAL N.V.** business and customer information from unauthorized disclosure, modification or loss.
- To establish safeguards to protect **BALKAN INTERNATIONAL N.V.** information resources from theft, abuse, misuse and any form of damage.
- To establish safeguards to protect **BALKAN INTERNATIONAL N.V.** equipment, network and applications.
- To establish responsibility and accountability for Information Security.
- To ensure that **BALKAN INTERNATIONAL N.V.** is able to continue business in the event of significant Information Security incidents.
- To ensure **BALKAN INTERNATIONAL N.V.** compliance with applicable laws and regulations and industry best practices.
- To encourage management and employees to maintain an appropriate level of awareness, knowledge and skill to allow them to minimize the occurrence and severity of Information security incidents.
- To protect the confidentiality, integrity and availability of all company's business information to safeguard the company's assets, stakeholders and reputation, irrespective of its form
- To establish safeguards to protect **BALKAN INTERNATIONAL N.V.** Business, information resources and equipment from an Intrusive computer software (such as computer viruses)

BALKAN INTERNATIONAL N.V.IT Security Governance and Management

BALKAN INTERNATIONAL N.V. Executive Board is responsible for the Information Security Policy. The board has delegated the day-to-day operation of Information Security to the Information Security Officer (ISO).

Information Security Officer (ISO)

The ISO is responsible for ensuring that the Information Security Policy is implemented in **BALKAN INTERNATIONAL N.V.** business operations. The ISO is also responsible for all day to day Information Security issues and is the first point of contact for all security related issues within the organization. The ISO may delegate some or all of the policy sections but is ultimately responsible for its implementation.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Companies contracted to **BALKAN INTERNATIONAL N.V.** found to be violating this policy will be deemed to be in breach of contract.

Revision and Changes

All **BALKAN INTERNATIONAL N.V.** procedures are subject to an annual revision, which has to be completed before the annual financial audit of the company. Significant changes to any policy or procedures are to be approved by the Key Official and communicated to the MGA.

Security Policy

- The function of an Information Security Officer shall be fulfilled by a person within the organization or its subsidiaries and shall be appointed by the Executive Board. This function must be fulfilled at all times. The position of the ISO shall be independent from other functions of the organization and shall be part of the department responsible for Corporate Governance.
- An Information Security Management Committee composed of senior managers should meet quarterly to review the current status of **BALKAN INTERNATIONAL N.V.** Information Security, approve new or modified security policies and other high-level security management activities. The first meeting is to be held 30 days from the first customer intake.
- The ISO must compile and maintain a list of contacts in authorities such as law enforcement, Malta Gaming Authority, the Financial Intelligence Analysis Unit (Malta), emergency services, health & safety and services providers.
- The ISO must maintain contact with special interest groups or other specialist security forums and professional associations which deal with information security.

- A periodic independent review of **BALKAN INTERNATIONAL N.V.** approach to managing information security and its implementation shall be commissioned by the ISO.
- The ISO must strive to find ways how to make the information security policy easy available to staff.
- The ISO must ensure that all contracts and agreements with 3rd parties comply with **BALKAN INTERNATIONAL N.V.** security policies and include appropriate Non-Disclosure Agreements (NDA's).
- A set of Information Security Policies, of which this document is one, should be written, agreed and communicated to all employees and third party organizations so that security requirements and obligations are well understood by all concerned.

Classification of Information Storage for Security Purposes

A Separate Policy called **Data Classification Policy** shall be published by the ISO to identify the Information's level of sensitivity and degree of protection that need to be applied.

In broad terms, Information shall be stored in electronic or hardcopy means. In the case of information stored on electronic media, storage shall be subdivided into live data and archived data which refers to instantly accessible information and to off-line storage.

BALKAN INTERNATIONAL N.V. Assets for Information Storing

The Department Managers shall inform the ISO of all assets that store information within their department whether in electronic or hardcopy format. Managers must also inform the ISO of assets that are capable of holding information (such as hard disks on desktop computers) which may not necessary be holding information related to the business of the organisation, but are used to process it or used as temporary storage (such as USB keys).

The ISO shall maintain an asset register where Information is stored within the organisation. The ISO shall be responsible to ensure that the information is being captured, processed and stored according to the data classification policy and the Personal data protection policy.

Access to Information

The ISO is responsible to formulate a list of different categories of access rights to the Remote Gaming system and the Control System and keep it updated. Similarly, a classification list of persons who have access to information within the organisation must be kept by the ISO. Access to the **BALKAN INTERNATIONAL N.V.** Remote Gaming System shall be categorized into types of users having different access rights. The ISO shall approve new categories.

- All sensitive information whether in electronic or hard copy format must be marked as "Confidential".
- Any information that is addressed to a particular person must be marked "Private".

Physical & Environmental Security

Objective

To prevent unauthorized physical access to or damage and interference with **BALKAN INTERNATIONAL N.V.** information assets.

Scope

Applies to all the buildings and facilities owned or operated by **BALKAN INTERNATIONAL N.V.** In case of information held by third parties the ISO shall ensure that the service provider adheres to these policies.

Policy

- Physical security barriers, such as card-controlled entry systems, must protect both the production and office environments.
- Buildings and equipment must be protected against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disasters.
- Public access areas such as delivery and loading areas must be controlled and isolated from the information processing facilities.
- All users should be given a unique user identifier, preferably common across all systems if access to multiple systems is required.
- It must be possible to track the access rights and privileges granted to individual users. The ISO must periodically review these access rights and privileges using a formal process.
- Generic accounts must only be used when there is demonstrably no alternative, and all generic accounts used should be recorded by the ISO, together with a list of individuals who have access to the generic accounts.
- All user passwords must be changed every 60 days and be a minimum of 8 characters. At least one character must be alphabetic and at least one character must be numeric or a symbol/punctuation character. This policy must be enforced where possible at the Operating System level.
- All production database systems must be configured with strong access controls and there must not be any vendor-supplied defaults in the production environment.
- The production application must strongly authenticate to the production database in a way that cannot also be used for unauthorized interactive access.
- The production application authentication to the production application must not use the same credentials that are also used elsewhere (i.e. in any test or staging environment).
- There must be a formal employee / contractor ("User") registration and deregistration procedure in place or granting and revoking access to all information systems and services within **SKILROCK TECHNOLOGIES MALTA LIMITED**
- All critical production and office environment equipment must be protected and maintained:
 - Power failure protection (UPS)
 - Heating, Ventilation and Air-Conditioning (HVAC) provision and failure protection
 - Cable duct protection for power and telecoms lines
- All equipment must be correctly operated and maintained to ensure its continued availability and integrity of maintenance and support agreements.

- Equipment containing any form of media storage must be securely disposed of at end-of-life. A set of procedure to Decommission Equipment shall be made available to technical staff and a Destruction of Sensitive Information Procedure shall be issued to all staff.
- Equipment must not be taken off-site without prior authorization.

Communications & Operations Management

Objective

To ensure the correct and secure operation of information processing facilities.

Scope

Applies to all **BALKAN INTERNATIONAL N.V.** information processing facilities.

Policy

General

- All communications whether printed or sent electronically must have a non disclosure statement.
- Printed sensitive information that is to be communicated across the organisation must be placed in a sealed envelope and marked “**CONFIDENTIAL**”.
- Operating procedures should be documented, maintained and made available to all users who need them.
- Operating procedures and documentation must also be made available in Escrow so that they would still be accessible to **BALKAN INTERNATIONAL N.V.** in the event of business failure of the hosting company or other 3rd party.
- As far as practical, duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or accidental modification or misuse of **BALKAN INTERNATIONAL N.V.**'s assets.
- All 3rd party service definitions and delivery levels (Service Level Agreements or SLA's) should be included in the legal contracts and agreements and monitored for compliance.
- Production application resource usage should be monitored, tuned and projections made of future capacity requirements.
- Acceptance criteria for all systems should be established and suitable tests of the systems carried out during development.

Backups

- All production server systems must be regularly backed-up using a standard backup methodology (e.g. Grandfather, Father and Son) and backup media must regularly be transferred and stored off-site.
- Sensitive data must be encrypted both on disk and on the backup media and be capable of authorized decryption for at least as long as required for regulatory compliance (currently 10 years).
- Backup systems must be periodically tested with a restore operation to ensure that the procedure works as expected.
- Backup media must be archived for the minimum period for regulatory compliance (currently 10 years).
- Backup media holding sensitive information must be marked with the words “**Confidential**”.

Information Systems Acquisition, Development & Maintenance

Objective

To ensure that security is an integral part of information systems.

Scope

This policy applies to all information and systems within the **BALKAN INTERNATIONAL N.V.** infrastructure.

Policy

General

- Business requirements for new information systems or enhancements to existing systems must specify the requirements for security controls.
- Data and databases used in test or staging environments must be sanitized and not contain any sensitive or confidential information.
- The ISO must maintain an awareness of new security vulnerabilities as they are discovered and assess the impact on the production and office environments.
- The production and office environments should be regularly audited for compliance with security policy and also initially audited before go-live.
- The production and office environments should be regularly penetration tested by a 3rd party, on at least an annual basis and initially before go-live.

Production Environment

- All production environments must be designed and operated in a multiply redundant configuration so that there is no single point of failure in the production infrastructure.
- All production systems must be subject to a level of operating system hardening and not running any unnecessary services.
- All production systems must have a patch program in-place to identify any software patches required and install them as required.
- The production environment must not contain components with known vulnerabilities unless a risk assessment has been made and signed-off by the ISO.

Application Design

- Application software must be robust, self-checking, and not vulnerable to invalid user input or the deliberate or accidental corruption of information.
- All production applications must protect the confidentiality and integrity of the data that they use or rely on.
- All production applications must follow the latest version of PCI guidelines for the development of secure web applications. The ISO shall be responsible in ensuring that the latest version of the PCI guidelines are communicated and understood by all developers.
- The production application must not be vulnerable to a simple Denial of Service attack such as an automated "first page" player registration.
- The production application must generate a secure audit trail of all activity which is digitally signed by the application and can be shown to be unmodified in a Court of Law.

- The application software must validate all customer-requested data changes by sending an automated email to the customer. This email must be responded to by the customer before the requested change to customer data can be made.
- The application must be able to reliably determine the country of origin of a player during the sign-up operation.
- The application must take all possible steps to ensure that player sign-up is legal in the country of origin of the player.
- The application web site must comply with common content-rating guidelines so that it can be blocked, if required, by relevant authorities.
- The application must comply with all relevant data protection legislation, particularly with regard to personal data.

Source Code

- Access to the application source code must be restricted to authorized individuals only and the source code must be encrypted outside the office environment (Laptops etc.)
- Application source code must not contain embedded authentication credentials.
- Application source code must not be held on any systems in the production environment, and
- An independent trusted 3rd party must review the production code to ensure that there is no functionality present which is not documented.
- Production environment or source code changes must be logged using a formal change management system and be subjected to peer review and approval before being released into the staging or test environment.
- Production environment changes must always contain an approved back-out plan in the event of unforeseen consequences of the change.
- Release of code from the staging environment to the live production environment must involve multiple levels of sign-off and agreement.

Data Security

- Data Backup and Retention

Back up copies of data and software associated with restricted or essential electronic information resources must be sufficient to satisfy disaster recovery requirements, application or other Electronic Information Resource processing requirements, and any functional requirement of any Electronic Information Resource Proprietor dependent upon such data Backup copies of Essential data for Disaster Recovery purposes must be stored at a secure, commercial site that provides standard protection or at a non-commercial off-site providing equivalent protection. These backup requirements extend to essential or restricted software and data stored on personal computers as well as software and data stored on shared servers.

- Data Privacy

Company electronic information resources must conform to company policies and regulations related to privacy of data or information records associated with them.

- Transferring and Downloading Data

The electronic information resource proprietor must ensure that the authorised user has implemented appropriate security measures before any restricted data is transferred to the

destination system. Security measures on the destination system must be electronic information recourse proprietors for restricted data must ensure that authorized users are apprised of this constraint when access is originally requested by the authorized user. The electronic information resource proprietor may choose to require the authorised user signature to acknowledge this notification.

- Encryption

Encryption is an important tool for protecting the confidentiality of sensitive or business-critical information when physical security cannot be provided. Encryption measure can be applied to information in transit across a communication system and/or in storage on computer readable media. Encryption of information in transit across communication system protects information from observation during transmission.

Encryption of storage protects information from being accessed when an unauthorised individual gains physical access to the device. Although encryption may serve as a surrogate for physical security, it is not a replacement for other appropriate logical security measures.

Suitably strong encryption measures employed and implemented with appropriate assurance can prevent the disclosure of electronic information to unauthorised parties;

However, encryption of information in storage presents risks to the availability of that information. Therefore, the use of encryption must take into account the nature of the resource and the company requirements for the timely or continued availability of the information.

- Transit

Wherever deemed appropriate, restricted data should be encrypted during transmission using encryption measures strong enough to minimise the risk of the data's exposure if intercepted or misrouted. In order for the transmission and decryption to be ready, the recipient must have access to appropriate encryption measures. A secure method must be used to convey the decryption measure to the recipient. Choices may include a public key infrastructure or a separate communication that includes verification of the identity of the recipient. The information must be decrypted upon receipt at its destination, as necessary, to conform with the storage requirements below.

- Storage

Records subject to disclosure must be available to appropriate company officials at all times. Other information that may be required to conduct company business must also be stored in a known location in unencrypted form or, if encrypted, the means to decrypt it must be available to more than one person, such as the electronic information resource proprietor or custodian. The means to decrypt might include software and decryption keys, for example, and may be stored using an appropriate digital escrow method.

Where the company chooses to implement storage encryption, the implementing procedures must include an encryption key management plan. The company is advised to address the following conditions for appropriate cryptographic key management in their local key management plan:

The encryption key management plan must ensure that data can be decrypted when access to data is necessary. This required backup or other strategies to enable decryption, thereby ensuring that data can be recovered in the event of loss or unavailability of cryptographic keys.

The encryption key management plan must address handling compromise or suspected compromise of encryption keys. A contingency plan should address what actions should be taken in

the event of a compromise, such as with system software and hardware, cryptographic keys, or encrypted data.

Users must be made awarded of their unique role if they are given responsibility for maintaining control of cryptographic keys.

Management of encryption keys and key management software and hardware must be under the direct supervision of a company employee holding a critical position.

Firewalls and External Connectivity

Communications access controls, such as firewalls, must be present to limit unauthorized access to Restricted or Essential Electronic Information Resource across Company or Company communication networks. These firewalls maybe limited to protection at the appropriate subnet level.

- Intrusive Computer Software

While intrusive computer software (such as computer viruses) can potentially affect any type of computer or server, the area of greatest risk are personal computers that received files from external sources, whether over a network or dialup connecting, or via shared detachable storage devices.

The company should evaluate their exposure regarding adverse intrusive computer software for different information resources, and put in place precautions commensurate with the level of risk and the associated cost to the institution for such anticipated loss; and implement processes to notify users and take other appropriate remedial action in the event of propagation of intrusive computer software.

The company should designate a Company authority responsible for the coordination of tracking, taking preventive measures, and reacting to Intrusive Computer Software, such as computer viruses.

- Device Media Controls

The company should implement controls that govern the receipt, reuse, and removal of hardware and electronic media, including documentation of hardware reassignment, including controls to address the final disposition of hardware and electronic media and requirements that ensure complete removal of restricted data before disposition.

Departments must also consider physical security for personal computers and other local electronic information resources housed within their immediate work area or under their control, such as laptop computers, PDAs etc. Protection of physical equipment or of software and data residing on storage media, from theft, damage or improper use should be addresses. Particular attention must be paid where access to or functioning of restricted or essential electronic information resources is concerned.

Permanent copies of restricted data should not be stored for archival purposes on portable equipment such as laptop computers. Restricted data should one be stored temporarily on separate portable equipment such as laptops computers, and only for the duration of the necessary use. Restricted data may be retained on portable equipment only if protective measures, such as encryption, are implemented that safeguard the confidentiality or integrity of the data in the event of theft or loss of the portable equipment.

- Internet Use

Browsing Guidelines

Browsing should be limited to those sites that are required for the execution of Company business practices and research. The browsing of pornographic and other non-business related sites is strictly prohibited.

- Instant Messaging

The use of Instant messaging (IM) clients outside of direct business use is not permitted.

- Email

Legal Risks

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

If you send emails with any libelous, defamatory, offensive, racist or obscene remarks, you and the Company can be held liable.

If you forward emails with any libellous, defamatory, offensive, racist or obscene remarks, you and the Company can be held liable.

If you unlawfully forward confidential information, you and the Company can be held liable.

If you unlawfully forward or copy messages without permission, you and the Company can be held liable for copyright infringement.

If you send an attachment that contains a virus, you and the Company can be held liable.

By following the guidelines in this policy, users can reduce the legal risks involved in the use of email. If any user disregards the rules set out in this email policy, the user will be fully liable and the Company will disassociate itself from the user as far as is legally possible.

Legal Requirements

The following rules are required by law and are to be strictly adhered to: It is prohibited to send or forward emails containing offensive or disruptive content, which includes, but is not limited to defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify the IT team.

- Email Accounts

All email accounts on the company systems remain the property of the company.

- Personal Use

The company email system is for the use of legitimate business purposes. Therefore, users who send personal emails via this system should be aware that all of the email traffic going through the servers may be copied, read, distributed, supplied to third parties and/or deleted without the knowledge or permission of the mailbox recipient.

- Encryption

The sending of sensitive data via email should be performed with the use of secure encryption methods such as PKI.

Media and Equipment disposal policy

Purpose

The disposal of media, computer equipment, and computer software can create information security risks. These risks are related to the potential unauthorized disclosure of electronics, protected information or other sensitive data, violations of software license agreements, and unauthorized disclosure of intellectual property that could be stored in hard disks and other storage media.

This policy will govern the requirements of secure disposal of media containing sensitive data or protected information, by establishing a process through which the secure removal of sensitive data or protected information is achieved on all media used within **BALKAN INTERNATIONAL N.V.** prior to disposal.

Scope

This policy applies to all **BALKAN INTERNATIONAL N.V.** employees who authorize the disposal, handle the media or devices intended for disposal, or who are directly responsible for the disposal of media and devices containing sensitive data or protected information. This policy covers all fixed and removable storage devices owned by **BALKAN INTERNATIONAL N.V.** This includes, but is not limited to: magnetic media (including fixed disks, magnetic tape, floppy, and other removable drive disks), optical disks, non-volatile memory devices (including memory sticks and cards or USB memory storage), and PDAs. Any storage devices currently available, or that become available in the future due to new technology, are also covered by this policy.

Responsibility and requirements

Disposal and sanitation methods

- All electronic devices and media equipment, including storage media in personal computers and other hardware containing sensitive data or protected information, will be sanitized prior to disposal.
- The proper sanitation method depends on the type of media and the intended disposition of the media.
- Media containing sensitive data or protected information must be degaussed or destroyed prior to disposal so that data will not be retrieved and reused.
- Non-functioning and/or non-writable media containing sensitive data or protected information must be physically destroyed if degaussing or other sanitization is determined to be inadequate.
- Media not containing sensitive data or protected information can either be sanitized or destroyed to an appropriate condition.
- Disposal of media requires authorisation and tracking by the data owner of record.
- All methods of media disposal will be in agreement with information security best practices, while also considering cost-effectiveness and the safety of employees.

Office Responsibilities

- Each office will designate an individual(s) to be responsible for assuring that protected information, as well as the hardware or electronic media on which it is stored, is properly destroyed and cannot be re-created.
- Each office will designate an individual(s) to oversee the monitoring process.
- Each office will designate an individual(s) to document disposal information beginning with the point of designation for destruction to final disposal.
- The chain of custody of the data will be established and maintained in the disposal documentation and will clearly identify the asset or media to be disposed, as well as the individual(s) responsible for its disposal.
- Disposal information will be kept for a period to be specified by **BALKAN INTERNATIONAL N.V.**
- Each office will submit a report to the ISO on a semi-annual basis.

Policy and Procedure Updates

- Updates to Information Security policies concerning Media Controls will be made on a periodic basis.
- All employees responsible for disposal activities will receive periodic training on the use of software and tools utilised to prepare and audit media and devices for disposal.
- Disposal activities will be audited on a regular basis by a designated individual(s) to verify compliance.

Enforcement Authority

- The Information Security Officer (ISO) is the person designated to monitor and provide initial enforcement of **BALKAN INTERNATIONAL N.V.** information security program and policies.

Violations and Disciplinary Action(s)

- All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.
- The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to the responsible Director for appropriate action.
- As determined by the responsible Director, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO for further investigation.
- Employees or systems administrators or managers who wilfully or knowingly violate or otherwise abuse the provisions to this policy may be subject to: (1) disciplinary action as outlined by **BALKAN INTERNATIONAL N.V.**; or (2) criminal prosecution.

Definitions

- Degauss – To demagnetize data from storage devices in order to destroy the media so it is no longer usable.
- Device – Including but not limited to personal computers, laptops, handheld units (PDA's).
- Disposal - The final disposition of electronic data, and/or the hardware on which electronic data is stored.
- Employee - Individuals employed on a temporary or permanent basis by **BALKAN INTERNATIONAL N.V.** ; as well as contractors, contractor's employees, volunteers, and individuals who are determined by **BALKAN INTERNATIONAL N.V.** to be subject to this policy. For the purpose of this policy, this also refers to anyone using a computer connected to the **BALKAN INTERNATIONAL N.V.** network.
- Media Controls - Formal, documented, policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility.

Sanitization - The process of rendering data harmless

Information Security Incident Management

Objective

To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Scope

This policy applies to all information and systems within the **BALKAN INTERNATIONAL N.V.** infrastructure, its subsidiaries and service providers holding **BALKAN INTERNATIONAL N.V.** information on its behalf.

Policy

- A security incident handling procedure must be written and agreed with Operations staff. Roles and responsibilities must be clearly defined together with levels of action/response and escalation procedures.
- All **BALKAN INTERNATIONAL N.V.** employees, contractors and 3rd parties must be required to note and report any observed or suspected security weaknesses in systems or services.
- There must be a mechanism in place to enable the types, volumes and costs of information security incidents to be quantified and monitored.

Business Continuity Management

Objective

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

The production infrastructure for **BALKAN INTERNATIONAL N.V.**

- A managed process must be developed and maintained for business continuity that addresses the business and information security requirements needed for **BALKAN INTERNATIONAL N.V.** business continuity.
- Events that can cause interruptions to business processes must be identified, along with the probability and impact of such interruptions and their consequences.
- Plans must be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
- A single framework of business continuity plans must be maintained to ensure that all plans are consistent and to identify priorities for testing and maintenance.
- Business continuity plans must be tested and updated regularly to ensure that they are up to date and effective.

Compliance

Objective

To avoid breaches of any law, statutory, regulatory or contractual obligations.

Scope

This policy applies to all **BALKAN INTERNATIONAL N.V.** core operational processes.

Policy

- Statutory, regulatory and contractual requirements must be explicitly defined, documented and kept up to date.
- All intellectual property rights and licensing terms for the use of proprietary software products must be respected and enforced within **BALKAN INTERNATIONAL N.V.** and by all contractors and 3rd parties.
- Critical data must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements.
- Data protection and privacy must be ensured as required in relevant legislation, regulations and, if applicable, contractual clauses.
- Managers must ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.