

Information Security Policy

Table of Contents:

1. Introduction.....	3
About the Company	3
1.1. Purpose.....	3
1.2. Scope.....	4
1.3. Regulatory Compliance	5
2. Asset Management.....	6
3. Controls Against Malicious Software	7
4. Technical Vulnerability Management.....	8
5. Information Backup	9
6. Redundancy of Information Processing Resources	10
7. Event Logging and Monitoring	10
8. Network Control Mechanisms	14
9. Network Service Security.....	15
10. Web Content Filtering	16
11. Change Management.....	16
12. Access Control and Identity Management.....	17
13. Incident Management and Reporting	19
14. Roles and Responsibilities	20
15. Training and Awareness.....	21
16. Review and Updates.....	22
17. Continuous Improvement	22
18. Relation to Other Documents	23

1. Introduction

About the Company

Boni Holding is Bulgaria's largest pork producer and a key player in the food industry, supplying 30% of the country's fresh pork. The company primarily focuses on pig breeding and meat processing, complemented by its feed production operations, which support its breeding activities.

We operate seven pig farms for raising our livestock and have three feed production facilities dedicated to our animals. Our main meat processing center is situated in Lovech, featuring an industrial cutting house, a factory for production of salami and delicacies, and a factory for production of meat preparations (meat cuts, minced meats, raw sausages and semi-manufactured products; ready to eat/cook products). The close proximity of these three enterprises creates a highly efficient production complex.

Additionally, we have a unique facility for raw-cured products in Karlovo, known for its specialized microenvironment that imparts a distinctive flavor to our offerings. In 2021, we enhanced our business model by launching Bulgaria's most technologically advanced pig slaughterhouse in Targovishte, which plays a vital role in ensuring the high quality of our livestock throughout the meat processing chain.

Through our feed mills, pig farms, and meat production facilities, we ensure that our products meet the highest quality standards while contributing positively to the Bulgarian economy and society. Our mission is to provide Bulgarians with responsibly produced meat, ensuring care for people, animals, and the environment. To achieve this, we have set four strategic goals to shape the Company's development in the coming years and beyond:

- To increase the share of pork produced in Bulgaria in the consumption of Bulgarians (currently 2/3 of pork comes from Europe).
- To increasingly assert our leadership position and be the leading innovators in the meat industry.
- To respond to our customers' needs through scale and the ability to control more stages of production.
- To work to maintain the image of meat as a necessary food and to focus efforts in this direction.

1.1. Purpose

This Information Security Policy of Boni Holding is a foundational document that defines the framework and principles for protecting the organization's information and network assets.

The purpose of the Information Security Policy is to:

- Protect assets, networks, and systems from incidents, data loss, unauthorized access, and disruptions.

- Ensure the continuity of critical business processes, particularly in production and logistics.
- Establish clear roles, responsibilities, and procedures for the prevention, detection, and response to security incidents.
- Implement appropriate technical and organizational measures.
- Enhance Information Security awareness and culture among all employees and partners.

1.2. Scope

This policy applies to all divisions and enterprises within the structure of Boni Holding:

Pig farming division:

- Boni Farm Brestak AD
- Boni Farm Krumovo Gradishte AD
- Boni Farm Zimen AD
- Boni Farm Nikola Kozlevo AD
- Boni Farm Shumen AD
- Boni Farm Levski AD
- Boni Farm Pleven AD
- Boni Fodders Pordim EOOD

Meat Processing Division

- Boni Mesokombinat Lovech AD
- Boni Mesokombinat Karlovo AD
- Boni Mesokombinat Ruse AD
- Boni Marketing EOOD

The Information Security Policy also applies to:

- All IT and communication systems located within the territory of Bulgaria, including the company's 17 operational sites.
- All employees, external contractors, and suppliers who have access to systems and/or data.
- All assets, including servers, workstations, network devices, software systems, surveillance cameras, and controllers (including ERP and DVR systems).
- All processes related to access management, incident response, data backups, system updates, training, and other relevant activities.

1.3. Regulatory Compliance

The Information Security policy of Boni Holding is developed in accordance with the applicable legal framework in the field of network and information security, including but not limited to:

1.3.1. European Legislation

- Directive (EU) 2022/2555 (NIS2) – on measures for a high common level of Information Security across the Union. This directive expands the scope of regulated entities and strengthens requirements for risk management and incident reporting.
- Regulation (EU) 2016/679 (GDPR) – on the protection of personal data and privacy.
- Regulation (EU) 910/2014 (eIDAS) – on electronic identification and trust services for electronic transactions in the internal market.

1.3.2. National Legislation

- Information Security Act (promulgated in State Gazette No. 94/2018), updated to transpose the NIS2 Directive. It introduces new categories of entities ("essential" and "important") and mandates stricter Information Security measures and incident reporting obligations
- Ordinance on Minimum Requirements for Network and Information Security (MRNIS) – applicable to operators of essential services, setting both organizational and technical security standards.
- Personal Data Protection Act – aligning national data protection practices with GDPR.
- Penal Code and the Electronic Governance Act – particularly in sections addressing IT incidents and data misuse.

1.3.3. Best Practices and International Standards

The policy also aligns with recommendations from internationally recognized standards and guidelines, including:

- ISO/IEC 27001 – Information Security Management Systems (ISMS)
- ISO/IEC 27005 – Information security risk management
- ISO 22301 – Business continuity management systems
- ENISA (European Union Agency for Cybersecurity) – Guidelines and recommendations for implementing NIS2

The policy is implemented under the supervision of the Ministry of Electronic Governance (MEG), designated as the competent authority for enforcing NIS2 requirements for essential entities in the “Food Production and Processing” sector.

2. Asset Management

2.1. Definitions

An **asset** is any element that holds value for Boni Holding and may be subject to cyber threats, including:

- Hardware: Computers, servers, network equipment (firewalls, switches, routers), DVRs, controllers, printers, cameras, etc.
- Software: Operating systems (Windows, Windows Server), ERP systems, Microsoft 365, SIEM (Rapid7), antivirus (ESET), Veeam, etc.
- Data: Customer, production, commercial, HR, and financial information.
- Services: Cloud platforms, email systems, remote access, external APIs, etc.

2.2. Visibility and Control

Effective protection of Boni Holding’s information and operational infrastructure requires full visibility over all assets—hardware, software, network components, and information resources. This section defines the procedures and responsibilities for asset management.

2.3. Control Mechanisms

The selection of technological control mechanisms follows Clause 8 of Annex A of ISO/IEC 27001:2022. Implementation considers legal, regulatory, contractual, and other requirements to ensure a high level of information security and compliance of the ISMS with the standard.

2.4. End-User Device Policy

This policy applies to all employees and covers all data-processing devices regularly used in operations. These devices, when connected to Boni Holding’s systems and networks, fall under this policy to ensure the protection of any information stored, processed, or accessed through them.

2.5. Rules for Company-Owned Devices

The policy covers all types of stationary and mobile computers owned by Boni Holding. Key provisions include:

- **Physical Security:** Devices must not be left unattended in unsecured locations, public or private transport, or workspaces without supervision.
- **User Accounts:** Devices must be accessed via personal accounts to ensure secure authentication and authorization.
- **Backups:** Boni Holding does not maintain backups of personal computers or mobile devices.
- **Encryption:** All mobile computers must use encrypted file systems.
- **Access Restrictions:** Employees may not lend their devices to third parties or install/download unauthorized content or applications.
- **Clean Screen Policy:** Employees must lock screens when not in use and prevent shoulder surfing.
- **Information Storage:** A secure repository is provided for business data. By default, no business data should be stored locally on end-user devices to prevent unauthorized disclosure or loss.
- **Personal Data:** Storing personal or copyright-protected data on company devices is prohibited.
- **Network Access:** Devices not part of the domain group are prohibited from connecting to the internal network.
- **Operating Systems:** Only vendor-supported OS versions are allowed. Multiple supported versions may be used depending on licensing, hardware capacity, or upgrade feasibility.
- **Peripheral Devices:** Use of USB drives, portable internet cards, and other accessories is not prohibited.
- **Security Features:** Where technically feasible, devices must use UEFI boot and TPM 2.0. TPM 2.0 is mandatory for all new hardware acquisitions.

3. Controls Against Malicious Software

3.1. General Approach

Boni Holding implements effective tools and mechanisms for detecting and protecting against malicious software, along with appropriate procedures to maintain a high level of security awareness. Protection is based on:

- Security awareness
- Controlled access to systems
- Established change management practices

3.2. Implemented Control Mechanisms

Boni Holding has adopted the following measures to defend against malicious software:

- **Integrated Antivirus and Endpoint Detection & Response (EDR):** A comprehensive combination of ESET Antivirus and Rapid7 EDR is used to enforce security policies, centralized management, scanning, application control, portable device control, and network traffic monitoring.
- **File Scanning:** All email attachments and downloaded files are scanned for malware before use. This scanning occurs at multiple points: email gateways, server systems, desktop and mobile computers, and when messages enter Boni Holding's network.
- **Periodic System Scans:** Information systems, either partially or entirely, are regularly scanned for malicious software.
- **Tamper-Proof Protection:** It is not possible to disable the integrated software products responsible for malware detection and protection.

4. Technical Vulnerability Management

4.1. Guidelines for Managing Technical Vulnerabilities

To ensure effective control, the following procedures are followed when a potential technical vulnerability is identified:

- **Third-Party Responsibility:** Boni Holding has assigned a third-party partner with responsibilities for vulnerability management, including monitoring, risk assessment, remediation, asset tracking, and coordination.
- **Tools and Awareness:** Tools such as Rapid7 InsightVM and ESET are used to identify vulnerabilities and maintain awareness.
- **Alert Response:** The organization can respond to alerts about newly discovered vulnerabilities via the external Security Operations Center (SoC), internal IT teams, or security bulletins.
- **Risk Assessment and Remediation:** Upon detection of a potential vulnerability, the external SoC assesses associated risks and initiates corrective actions.
- **Urgency-Based Response:** Actions are prioritized based on the urgency and severity of the vulnerability, in line with security requirements.
- **Software Updates:** Risks associated with software updates are assessed. Updates are tested and evaluated before deployment in the production environment.
- **Alternative Controls:** If updates or firmware patches are not available, alternative controls are implemented:
- **Disabling vulnerable services or features**

- Reconfiguring or adding access control mechanisms
- Enhancing monitoring to detect or prevent attacks
- Increasing awareness of the specific vulnerability
- Audit Trails: Control records are maintained for certain procedures.
- Continuous Evaluation: The vulnerability management process is regularly monitored and evaluated to ensure its effectiveness.

4.2. Regular Inventory

All stakeholders—including Boni Holding’s internal team, IT service providers, and the external SoC—conduct regular asset inventories to maintain acceptable levels of technical vulnerability.

4.3. Security Compliance Monitoring

Security compliance is monitored by the external SoC in close collaboration with Boni Holding’s technical experts.

4.4. Security Assessment of New Systems

Before implementing new information systems or technical equipment, Boni Holding evaluates the security features provided by the manufacturer. A decision to implement is made only if the required security levels are met.

4.5. Post-Implementation Vulnerability Checks

After deployment, the external SoC conducts periodic checks to identify vulnerabilities and threats. Findings are reported to the responsible service provider or designated employee for remediation.

5. Information Backup

5.1. Backup Strategy

Boni Holding has implemented appropriate backup mechanisms to ensure that all critical information and software can be restored following a security incident. The backup and recovery process includes:

- Availability of Operational Data: Operational data stored and processed by systems is backed up using various technologies and storage locations, including Veeam, NAS, and Microsoft 365 Cloud. A backup schedule is maintained for systems identified as important or critical to business operations.

- **Work File Storage:** Work files from all local and portable systems must be saved in Microsoft 365 or another designated system. Files should not be stored on local employee drives. Employees are instructed that Boni Holding cannot guarantee the availability of files not stored in approved repositories.
- **Access Control:** Access to backup copies is strictly controlled.
- **Integrity Monitoring:** The integrity and quality of files stored in cloud services are monitored using built-in mechanisms to ensure reliability in emergencies.
- **Full Recovery:** The backup method ensures the restoration of all files, system configurations, and applications.
- **Recovery Responsibility:** Restoration is performed by the designated system administrator or service provider.
- **Testing:** Backup systems are tested at least once per year through trial restorations.
- **Group IT Systems:** Systems and data hosted by internal group IT providers are not subject to backup, testing, or management by Boni Holding.

6. Redundancy of Information Processing Resources

6.1. Single Point of Failure Analysis

Boni Holding conducts regular analyses to identify single points of failure or systems operating at maximum capacity. If such issues are found, immediate action is taken to resolve them. If resolution is not feasible within the current budget cycle, the associated risk is documented and accepted by management.

6.2. Cloud System Redundancy

Boni Holding uses cloud systems whose redundancy is guaranteed by the service provider. Management has accepted that the provider's uptime is sufficient to meet availability requirements. These cloud services typically maintain geographically distributed replicas, with automatic traffic rerouting in case of service disruption. This approach effectively ensures availability and redundancy when needed.

7. Event Logging and Monitoring

7.1. Log Retention

Cloud platform logs that record user actions, exceptions, and security breaches are maintained for a period of six (6) months. These logs serve as evidence in case of investigations and for monitoring access control.

7.2. Log Content

Control logs include the following information:

- Unique usernames or identifiers
- Geolocation of each successful login
- Date, time, and details of key events (e.g., system startup/shutdown)
- Identification of the endpoint device or location, where possible
- Records of successful and denied access attempts
- Records of successful and denied data/resource access attempts
- System configuration changes
- Use of privileged accounts
- Network addresses and protocols
- Activation and deactivation of security modules
- Unauthorized downloads or content sharing

7.3. Log Storage and Analysis

All logged events are stored in secure repositories. Boni Holding delegates the management of virtual storage, content control, and log analysis to an external Security Operations Center (SoC). Specialists are not permitted to delete, disable, or modify log entries.

Monitored areas include:

- Authorized Access: Unique user IDs, timestamps, event types, accessed files, and used applications/tools
- Privileged Operations: Use of administrator, specialist, or operator accounts; system start, restart, and shutdown
- Unauthorized Access Attempts: Failed or rejected user actions, data/resource access violations, access policy breaches, firewall alerts, and intrusion detection system warnings
- Security Configuration Changes: Attempts to alter security settings or control mechanisms

7.4. Log Protection

Mechanisms are in place to protect log data from unauthorized disclosure, modification, or deletion. Key protections include:

- Restricted access to logs
- Log content review is limited to the system manager and one designated specialist

7.5. Cloud Platform Logging

Management considers the logging capabilities of cloud platforms sufficient for tracking actions by system administrators, specialists, and operators. These logs include:

- Timestamp of successful or failed events
- Event or error details
- Involved accounts and responsible personnel

7.6. Log Retention in Rapid

Boni Holding retains log files containing records of user activity, exceptions, and security breaches in the Rapid7 system for a minimum of twelve (12) months. These logs serve as evidence for investigations and access control monitoring.

7.7. Log Content

Control records include:

- Unique usernames or identifiers
- Date, time, and details of key events (e.g., system startup/shutdown)
- Endpoint device or location identification, where possible
- Records of successful and denied access attempts
- Records of successful and denied data/resource access attempts
- System configuration changes
- Use of privileged accounts
- Network addresses and protocols
- Activation/deactivation of security modules
- Unauthorized downloads or content sharing

7.8. Log Storage and Management

All events are stored in secure repositories. Boni Holding delegates the management, content control, and analysis of these logs to an external Security Operations Center (SoC). Internal specialists are not authorized to delete, disable, or modify log entries.

7.9. Monitoring Focus Areas

Monitoring emphasizes:

- Authorized Access: User IDs, timestamps, event types, accessed files, and used tools
- Privileged Operations: Use of admin, specialist, or operator accounts; system start/restart/shutdown
- Unauthorized Access Attempts: Failed actions, policy violations, firewall alerts, and intrusion detection warnings
- Security Configuration Changes: Attempts to alter security settings or controls

7.10. Log Protection

Mechanisms are in place to protect logs from unauthorized disclosure, modification, or deletion. Key protections include:

- Restricted access to logs
- Log review is performed by a qualified external SoC specialist
- Boni Holding considers the information recorded in centralized local/cloud systems sufficient. Logs include:
 - Timestamp of successful or failed events
 - Event or error details
 - Involved accounts and responsible personnel

10.11. System and User Activity Monitoring

Boni Holding has implemented monitoring mechanisms for user and system activity, including:

- Inbound/outbound network, system, and application traffic
- Access to systems, servers, network equipment, surveillance systems, and critical applications
- Configuration files at critical or administrative levels
- Logs from security tools (antivirus, IDS, IPS, web filters, firewalls)
- Event logs related to system and network activity
- Resource usage (CPU, disk, memory, bandwidth) and performance
- Security baseline established for normal behavior; deviations are monitored
- Usage patterns during normal and peak periods
- Typical access times, locations, and frequency per user/group
- Behavioral indicators such as:

- Malware-related activity or traffic from known malicious IPs/domains
- Known attack patterns (e.g., DoS, buffer overflow)
- Abnormal system behavior (e.g., process injection, protocol misuse)
- Bottlenecks and overloads (e.g., network queueing, latency, jitter)
- Unauthorized access or scanning of systems, applications, or networks
- Successful/failed access attempts to protected resources (e.g., DNS servers, web portals, file systems)
- Unusual user/system behavior compared to expected norms

7.12. Incident Reporting

Abnormal events are logged as incidents and reported to relevant stakeholders after categorization and confirmation by the external SoC. The monitoring process aims to:

- Improve audit capabilities
- Enhance risk assessment
- Strengthen incident response
- Minimize the impact of adverse events
- Identify and reduce false positives that could obscure real threats to Boni Holding's operations

8. Network Control Mechanisms

8.1. Oversight and Agreements

Management regularly monitors its ability to manage internal network services and evaluates the capability of network service providers to securely deliver contracted services. Security agreements, service level requirements, management protocols, and audit rights are established. Boni Holding ensures that providers implement the agreed-upon security measures.

8.2. Key Network Security Features and Technologies

- Internet Connectivity – Managed routing devices are used to provide secure internet access across the organization.
- Virtual Private Networks (VPNs) – Boni Holding uses VPN technology to establish secure tunnels between its infrastructure and that of clients, suppliers, and employees. These tunnels are implemented using SSL VPN or IPSec, ensuring authentication and secure data transmission over untrusted networks.
 - IPSec Protocol is used for authentication and encryption.

- Remote access is initiated via a VPN client connecting to a network device (e.g., router or firewall).
- Authentication involves a unique username, password, and certificate, verified at each connection attempt.
- Successful authentication allows remote users to access resources within Boni Holding's local network.
- Data exchange with third parties may occur via SSL VPN or IPSec tunnels.
- Routing - Static routes are configured for managed network classes and subnets wherever applicable.
- Network Address Translation (NAT) - Boni Holding uses NAT to conceal the identity of internal resources. The implementation follows RFC1918, allowing the use of all private IP addresses defined in the standard.
- Email Security - Email communications are secured using TLS 1.3 encryption within Microsoft 365.

9. Network Service Security

9.1. Oversight and Agreements

Management regularly monitors its ability to manage internal network services and evaluates the capability of network service providers to securely deliver contracted services. Security agreements, service level definitions, management requirements, and audit rights are established. Boni Holding ensures that providers implement the agreed-upon security measures.

9.2. Key Security Features of Network Technologies and Parameters

- Internet Connectivity - Boni Holding uses Sophos XGS Firewall devices with all relevant subscriptions to manage internet connectivity across the organization.
- Wireless Communications - Wireless networks are based on IEEE 802.11n/ac/ax standards, operating on 2.4 GHz or 5 GHz frequency bands. Encryption is provided via WPA2 with AES 256-bit. Remote employees are instructed to use the same secure encryption protocols for wireless connections.
- Virtual Private Networks (VPNs) - VPNs are used to establish secure tunnels between Boni Holding's infrastructure and its clients or employees.
 - Implemented using SSL VPN and IPSec protocols
 - Ensures authentication and secure data transmission over untrusted networks
 - Remote access is initiated via a VPN client connecting to a firewall
 - Authentication involves a unique username, password, and certificate

- Successful authentication grants access to internal network resources
- Data exchange with third parties is supported via SSL VPN or IPSec tunnels
- Network Address Translation (NAT) - NAT is used to conceal internal resource identities. The implementation complies with RFC1918, allowing the use of all private IP addresses defined in the standard.
- Email Security - Email communications are encrypted using TLS 1.3 within Microsoft 365.

10. Web Content Filtering

10.1. Traffic Filtering

Traffic between systems and their subsystems is controlled through appropriate filtering mechanisms (e.g., by IP address, protocol, port number from the TCP/IP stack, etc.).

10.2. User Traffic Filtering

Mandatory filtering directions include:

- Blocking access to websites with poor reputations using NGFW (Next-Generation Firewall) and/or endpoint protection software installed on user devices
- Restricting web traffic from geolocations that are not typical for Boni Holding's operations
- Monitoring, analyzing, and blocking command-and-control (C2) servers associated with malicious activity
- Blocking access to websites with illegal content, such as torrent trackers and sites distributing unlicensed software

10.3. Port Management and Perimeter Monitoring

Unnecessary TCP and UDP ports are disabled through proper configuration of software solutions, hardware devices, and traffic control equipment. The company's IP perimeter is continuously monitored using specialized tools (e.g., Shodan) to alert stakeholders about newly exposed or modified services/ports.

11. Change Management

11.1. General Principles

All changes related to information processing facilities and systems are documented and managed. Boni Holding aims to prevent unauthorized changes to minimize security risks. Responsibilities for change management are clearly defined, and mechanisms are in place to ensure effective control over significant changes to infrastructure, hardware,

communication systems, operating systems, software applications, business processes, procedures, and technologies.

11.2. Change Management Process

The process includes:

- Change Requests: Initiated by employees or clients via the ticketing system (support.baselineit.eu) or email to management. Requests are reviewed by the Manager, who decides on approval, timing, and execution.
- Triggers for Change (not limited to):
 - Implementation or reconfiguration of critical hardware
 - Deployment or upgrade of operating systems
 - Deployment or upgrade of business applications
 - Modifications to established procedures
- Assignment: Changes are assigned by the Manager to qualified specialists or third parties under contract.
- Execution Oversight: The Manager oversees implementation.
- Documentation: Approved changes are recorded in a dedicated database with controlled and traceable access.
- Change Records Include:
 - Description of the change
 - Planned action
 - Expected and actual results
 - Approval status
 - Acceptance or rejection of the new state
 - Rollback options to a stable previous state
- System Documentation: Updates may be reflected in related documents, diagrams, procedures, and systems.
- Notification: After successful implementation, responsible personnel must notify relevant stakeholders.
- Operational Changes: Only initiated when justified, such as introducing new functionality or addressing increased risk.

12. Access Control and Identity Management

12.1. Access Control Principles

Access control is a critical component of Boni Holding's security framework and is based on the principles of need-to-know and least privilege. Identity mechanisms are centrally managed by external partners to ensure traceability and control.

12.2. Centralized Identity Management

- User accounts are managed via Active Directory (on-premises) and Microsoft 365 (cloud), administered by an external IT partner.
- Access to cloud services is controlled through Azure Active Directory, synchronized with the local directory.

12.3. Identification and Authentication

- Each user is assigned a unique username and a personalized password.
- Multi-Factor Authentication (MFA) is mandatory for:
 - Microsoft 365
 - VPN connections and remote access
- Administrative accounts are separated from standard user accounts and are protected with additional security measures.

12.4. Password Management – Requirements

- Minimum of 12 characters
- Must include letters, numbers, and special characters
- Passwords must be changed every 90 days
- Reuse of the last 5 passwords is prohibited

12.5. Unified Password Policy

The password policy applies uniformly across all systems, including ERP, Active Directory, local servers, and cloud services.

12.6. Role-Based Access Control (RBAC)

- Group membership in Active Directory defines access levels to resources.
- Permissions are assigned based on job roles (e.g., Operator, Accountant, Site Manager, IT Admin).
- Access to critical systems (ERP, file servers, SIEM) is restricted to authorized personnel only.

12.7. Access Management for External Providers

- External IT providers and the SoC have strictly limited administrative access, governed by contract and security policy.
- Access is time-bound and monitored in real-time via the SIEM system.

13. Incident Management and Reporting

13.1. Strategic Approach

Boni Holding considers incident management a key component of its Information Security framework. The objective is to ensure timely detection, escalation, analysis, response, and recovery from events that threaten:

- Information assets
- Business continuity
- Data confidentiality

In alignment with the NIS2 Directive and national regulatory requirements, an Incident Response Plan (IRP) is established.

13.2. Definition of a Security Incident

A ***security incident*** is defined as any event that:

- Compromises or has the potential to compromise:
 - Confidentiality
 - Integrity
 - Availability of systems, data, or services
- Disrupts production or IT processes
- Leads to:
 - Unauthorized access
 - Abuse of privileges
 - Data breaches
 - Fraud
 - Data leakage

13.3. Roles and Responsibilities

- SoC Partner - 24/7 monitoring, alerting, initial analysis, and first-level response actions

- IT Partner – Technical support, access blocking, recovery, and log inspection
- Chief Executive Officer – Approval for notifying the Ministry of Electronic Governance (MEG), strategic decision-making
- MEG Contact Person- Notification within 24 hours of identifying a major incident

13.4. Incident Management Process

- Detection – via SIEM (Rapid7 InsightIDR) or reports from staff/service providers
- Assessment – SoC analyzes scope, impact, and severity
- Escalation – CEO is notified
- Response – affected services are halted, access is blocked, and impacted parties are informed
- Recovery – restoration from backups (Veeam), cleansing of affected assets
- Documentation – incident report, lessons learned, and follow-up actions

13.5. Notification to Supervisory Authority

- For incidents classified as significant, Boni Holding must notify the Ministry of Electronic Governance (MEG) within 24 hours of detection.
- The report must include:
 - Nature of the incident
 - Affected assets
 - Time of detection and response
 - Actions taken
 - Potential consequences
- Within 72 hours, Boni Holding, with support from its partners, must identify all affected parties and submit this information to MEG as per its procedures.
- Within 30 days, Boni Holding must submit a final report to MEG, including conclusions and digital artifacts discovered during the investigation. If no further action is required, the incident is considered resolved.

14. Roles and Responsibilities

➤ Chief Executive Officer (CEO)

- Approves the Information Security policy and related plans
- Makes strategic decisions in case of major incidents or breaches
- Allocates budget and sets security priorities

- Approves training plans and funds training initiatives
- **External Security Operations Center (SoC) Provider**
 - Provides 24/7 system monitoring via Rapid7 InsightIDR
 - Analyzes incidents, responds, and issues notifications
 - Manages vulnerabilities using InsightVM
 - Offers security consulting and technical support
- **External IT Providers**
 - Manage Active Directory, Microsoft 365, ERP systems, and runZero
 - Install, update, and maintain endpoints and servers
 - Maintain network infrastructure
- **Employees and Operators**
 - Comply with policies and internal regulations
 - Participate in mandatory training
 - Report suspicious incidents or behavior
- **Expert Personnel**
 - Future roles will be assigned, including: CISO / DPO / internal IT coordinator for operational control and coordination with external providers

15. Training and Awareness

15.1. Strategic Importance

Boni Holding recognizes that employees are both its most valuable asset and a potential vulnerability in the context of information security. Therefore, the organization adopts a systematic approach to training and awareness to ensure all employees can recognize risks and respond appropriately to suspicious situations.

15.2. General Policy

All employees with access to information assets are required to complete annual Information Security training, delivered by an external partner or through an e-learning platform.

New hires must complete onboarding Information Security training within the first 30 days of employment.

15.3. Training Topics

- Information Security fundamentals
- Social engineering and phishing attacks
- Password policies and access protection
- Safe handling of emails and documents
- Secure use of devices and the internet
- Incident response procedures
- Responsibilities when handling sensitive information (including personal data)

15.4. Training Methods

- Online platforms with quizzes and assessments
- In-person seminars or workshops
- Simulated phishing campaigns
- Role-based incident response exercises (drills)

15.5. Documentation and Compliance

- A training register is maintained, recording dates, participant names, and test results
- Management and the SoC monitor compliance and training frequency
- Failure to complete training may result in restricted access to information assets

16. Review and Updates

The policy is reviewed and updated at least once per year, or whenever there are significant changes in legislation, technology, or business processes.

The Information Security Officer (currently represented by the external SoC) is responsible for conducting the review and making recommendations.

The Policy becomes effective from the date of signature and is mandatory for all employees, partners, and service providers with access to the company's information systems.

Boni Holding is committed to regularly review the Information Security Policy as to ensure ongoing compliance with relevant EU and national legislation and implementation of best practices in the field.

17. Continuous Improvement

Boni Holding is committed to ensuring the resilience and predictability of its IT-dependent production processes and business operations. Achieving this requires the implementation

of new technologies, cybersecurity tools, services, and documentation aligned with the organization's risk assessment.

We have set the following Key Strategic Goals:

- Implement an effective and efficient cybersecurity management process in compliance with the *Ordinance on Minimum Requirements for Network and Information Security (MRNIS)*.
- Ensure cyber resilience through the deployment of carefully selected security tools and technologies.
- Reduce the risk of cybersecurity incidents by continuously monitoring and analyzing the behavior of information systems and users.
- Achieve readiness for incident detection, reporting, and response, minimizing potential damage.
- Manage known and emerging vulnerabilities by improving the effectiveness of response measures or introducing new ones.
- Clearly define and separate roles and responsibilities related to security and IT process management within Boni Holding.
- Conduct informed risk assessments, followed by treatment plans aimed at achieving measurable improvements.
- Ensure targeted and efficient use of public funds to support cybersecurity and IT operations.
- Outsource activities for which Boni Holding lacks the necessary internal expertise.
- Document and regularly update responsibilities, activities, and processes related to IT operations and cybersecurity.
- Support business objectives by implementing effective security measures that ensure the continuity of IT-dependent processes.
- Introduce a service management process for services provided by Boni Holding to its students, with resilience and security as key success indicators.

18. Relation to Other Documents

- Contractual clauses on Information Security with suppliers and clients
- Ordinance on Minimum Requirements for Network and Information Security (MRNIS)
- Internal procedures, instructions, and regulations
- Risk Assessment Policy (conducted in full compliance with MRNIS)

Version number	Approver	Periodic review date	Performed by	Next review date
1.0	Board of directors decision dated 05.06.2025			01.07.2026
2.0	Board of directors decision dated 05.06.2026			01.07.2028

