

NewEra B.V.
Information Security Policy

20.04.2026

1. Introduction and Purpose

NewEra is committed to establishing, maintaining, and continuously improving an effective information security framework designed to protect its information assets, technology infrastructure, and operational processes against internal and external threats.

This Information Security Policy defines the overarching principles, objectives, and control environment through which NewEra safeguards the confidentiality, integrity, and availability of all information processed, stored, or transmitted within its operations. It provides the foundation for the Company's approach to identifying, managing, and mitigating information security risks, and serves as a central reference point for all related procedures, standards, and controls implemented across the organization.

As an igaming operator, NewEra operates in an environment where the protection of sensitive information is critical to maintaining trust, ensuring fair gaming practices, and preserving the stability and integrity of its platform. The Company's activity involves player data, financial transactions, and operational information, all of which require a high level of protection against unauthorized access, misuse, disclosure, alteration, or loss.

In this context, NewEra recognizes that information security is not solely a technical function, but an integral component of its overall governance, risk management, and compliance framework. Accordingly, this Policy is designed to address a broad range of risks, including but not limited to cyber threats, fraud, insider misuse, human error, system vulnerabilities, third-party dependencies, and service disruptions.

The objectives of this Policy are to ensure that:

- Information is protected in a manner proportionate to its sensitivity;
- Security controls are implemented consistently across systems, processes, and third-party arrangements;
- Risks are identified, assessed, and managed in a structured manner;
- Incidents are detected, reported, and resolved effectively;
- The Company remains compliant with applicable legal and regulatory requirements.

This Policy aims to promote a culture of security awareness and accountability across NewEra, ensuring that all personnel understand their responsibilities in protecting information and supporting the Company's security objectives.

2. Scope and Applicability

This Policy applies to all information assets, systems, and operational processes that are owned, operated, or otherwise managed by NewEra, whether these are maintained internally or through third-party service providers. The scope of this Policy is intended to be comprehensive and extends across all areas of the Company's business activities where information is created, processed, stored, transmitted, or otherwise handled.

The Policy applies to all personnel acting on behalf of NewEra, including employees, contractors, consultants, and any other individuals granted access to Company systems or data. All such individuals are required to comply with the principles and controls defined herein as a condition of their engagement with the Company. This includes adherence to security requirements when accessing Company systems remotely, using personal devices where permitted, or interacting with third-party platforms integrated into NewEra's operations.

From a systems perspective, the scope of this Policy encompasses all technology environments that support the Company's services. This includes, but is not limited to, the gaming platform, player account management systems, payment processing systems, back-office and administrative tools, internal communication platforms, and supporting infrastructure such as servers, databases, networks, and cloud-based services. Both production and non-production environments, including development, testing, and staging systems, fall within the scope of this Policy, recognizing that vulnerabilities in any environment may impact overall security.

The scope of this Policy also extends to all categories of data handled by NewEra. This includes player personal data, identity verification (KYC) information, financial and transactional data, gaming activity records, authentication credentials, and internal business information. Data is considered in scope regardless of its format, including electronic records, system logs, backups, and any physical records where applicable.

In addition, this Policy applies to all third-party relationships that involve access to NewEra systems or the processing of NewEra data. This includes service providers such as hosting and cloud infrastructure providers, gaming platform providers, payment service providers, identity verification providers, software developers, and support vendors. NewEra recognizes that third-party dependencies introduce additional risk and therefore requires that such providers operate in accordance with security standards consistent with this Policy.

The controls outlined in this Policy apply across all geographic locations and operational contexts in which NewEra conducts its business. Where local legal or regulatory requirements impose additional or more stringent obligations, those requirements shall take precedence, and this Policy shall be interpreted and applied in a manner that ensures compliance.

This Policy should be read in conjunction with any supporting procedures, standards, and internal guidelines that provide further detail on specific control areas. Together, these documents form an integrated framework that ensures information security is managed consistently, effectively, and in alignment with the Company's risk profile and regulatory obligations.

3. Governance and Security Framework

NewEra maintains a structured and integrated governance framework to ensure that information security is effectively managed, appropriately resourced, and continuously aligned with the Company's operational and regulatory requirements. Information security is embedded within the broader corporate governance and risk management structure and is treated as a critical business function rather than a purely technical discipline.

Ultimate accountability for information security rests with the Management, which is responsible for establishing the Company's risk appetite, approving this Policy and any material updates, and ensuring that adequate resources, systems, and oversight mechanisms are in place to support its effective implementation. The Company Management also ensures that information security considerations are incorporated into strategic decision-making, including the adoption of new technologies, engagement of third-party providers, and expansion of business operations.

The Compliance Team is responsible for the design, maintenance, and ongoing development of the information security framework. This includes establishing policies and procedures, conducting risk assessments, monitoring the effectiveness of controls, and ensuring that the Company's practices remain aligned with applicable legal, regulatory, and licensing requirements. The Compliance Team also plays a key role in coordinating internal reviews, supporting audits, and facilitating communication between operational teams and management in relation to security risks and control effectiveness.

The Tech Team is responsible for the implementation and day-to-day operation of technical security controls across the Company's systems and infrastructure. This includes managing access controls, maintaining system configurations, implementing protective technologies, monitoring system activity, and responding to technical security events. The Tech Team ensures that systems are designed, configured, and maintained in a manner that supports the Company's security objectives and minimizes exposure to vulnerabilities.

Information security responsibilities are further integrated into operational processes across all teams within NewEra. Personnel are required to act in accordance with established security procedures, to exercise due care when handling information, and to report any actual or suspected security incidents or weaknesses without delay. This collective responsibility supports

a culture in which information security is recognized as a shared obligation across the organization.

The governance framework also incorporates mechanisms for oversight, review, and continuous improvement. Information security risks, incidents, and control effectiveness are periodically reported to the Management Team to ensure appropriate visibility and decision-making. Internal reviews are conducted to assess the adequacy of controls, and where necessary, corrective actions are implemented in a timely manner.

4. Risk Management Approach

NewEra adopts a structured, risk-based approach to the management of information security, recognizing that effective protection of its systems and data requires continuous identification, assessment, and mitigation of risks in a manner proportionate to their potential impact on the business.

The Company maintains a formal risk management process that is integrated into its overall governance and operational framework. This process is designed to ensure that information security risks are systematically identified across all areas of the business, including technology infrastructure, operational processes, personnel activities, and third-party relationships. Particular consideration is given to risks inherent in the online gambling environment, including threats to player accounts, financial transactions, platform availability, and the integrity of gaming operations.

Risk identification activities consider a broad range of threat scenarios, including but not limited to cyberattacks such as unauthorized system access, distributed denial-of-service (DDoS) attacks, malware infections, and ransomware incidents; fraud risks including payment abuse and account takeover; insider threats arising from misuse of privileged access; and operational risks such as system failures, misconfigurations, and human error. Risks associated with third-party providers, including hosting, platform, and payment services, are also assessed as part of this process.

Once identified, risks are evaluated based on their likelihood of occurrence and the potential impact on NewEra's operations, financial position, regulatory compliance, and reputation. This assessment allows risks to be prioritized and ensures that resources are allocated effectively to address those risks that pose the greatest threat to the business.

All identified risks are documented in a centralized risk register, which is maintained as a living record of the Company's risk profile. Each risk entry includes a description of the risk, its assessed severity, the controls currently in place, and any additional mitigation actions required.

Responsibility for implementing mitigation measures is assigned to the relevant team, and progress is monitored to ensure timely resolution.

Risk assessments are conducted at least annually and are also triggered by significant changes within the business, such as the introduction of new systems or technologies, changes to operational processes, onboarding of new third-party providers, or the occurrence of material security incidents. This ensures that the risk management process remains dynamic and responsive to the evolving threat landscape.

The Compliance Team oversees the risk management process, ensuring that assessments are carried out consistently and that findings are reported to the Management Team. Regular reporting provides visibility into the Company's risk exposure and supports informed decision-making at the management level.

5. Access Control and Identity Management

NewEra maintains a comprehensive access control framework designed to ensure that access to systems, applications, and data is granted only to authorized individuals and strictly limited to what is necessary for the performance of their duties. This framework is based on the principles of least privilege, need-to-know, and segregation of duties, and is implemented consistently across all environments and systems within the Company's operational scope.

Access to NewEra systems is provisioned through a controlled and documented process. All access requests must be formally submitted and approved prior to implementation, with approvals granted based on clearly defined roles and business requirements. The Tech Team is responsible for implementing access rights in accordance with approved requests, ensuring that permissions are aligned with the user's role and responsibilities.

User accounts are uniquely assigned and are not shared between individuals, ensuring accountability and traceability of all actions performed within Company systems. Authentication mechanisms are designed to provide a high level of assurance, with multi-factor authentication enforced for access to administrative functions, critical systems, and any environment containing sensitive data. Password controls are implemented in line with industry best practices, including requirements for complexity, periodic updates, and secure storage.

Privileged access, including administrative and system-level permissions, is subject to enhanced controls due to the elevated risk associated with such access. These accounts are restricted to a limited number of authorized personnel, are granted only where strictly necessary, and are closely monitored. Activities performed using privileged accounts are logged in detail and are subject to periodic review to detect any unauthorized or inappropriate use.

The Company maintains processes for the timely modification and revocation of access rights. Access is reviewed periodically to ensure that permissions remain appropriate to the user's role, and any unnecessary or excessive access is removed. In cases of role change or termination, access rights are adjusted or revoked promptly to prevent unauthorized access.

Access to systems is continuously logged, and these logs are retained and protected to ensure their integrity. Monitoring processes are in place to identify unusual or suspicious access patterns, enabling timely investigation and response where necessary.

6. Data Protection and Information Handling

NewEra implements a comprehensive framework for the protection and proper handling of information, recognizing that the secure management of data is fundamental to maintaining trust, ensuring regulatory compliance, and safeguarding the integrity of its operations. This framework is designed to ensure that all data is protected against unauthorized access, disclosure, alteration, or loss throughout its lifecycle.

All information processed by NewEra is classified according to its sensitivity and criticality to the business. This classification determines the level of protection applied and ensures that appropriate controls are consistently implemented. Particular emphasis is placed on the protection of sensitive data, including player personal information, identity verification documentation, financial and transactional records, authentication credentials, and internal business data.

Data is handled in accordance with defined security principles, including the minimization of data collection to what is necessary for legitimate business and regulatory purposes. Access to sensitive data is restricted to authorized personnel based on their role and business need, and is governed by the access control framework described in this Policy.

To protect data in transit, NewEra utilizes secure communication protocols and encryption standards to prevent interception or unauthorized disclosure. Where appropriate, sensitive data is also protected through encryption at rest, ensuring that it remains secure even in the event of unauthorized system access. Additional safeguards, such as tokenization, hashing, or masking techniques, may be applied to further reduce exposure of critical data elements.

Data retention practices are defined in alignment with legal, regulatory, and operational requirements. Information is retained only for as long as necessary to fulfill its intended purpose, after which it is securely archived or permanently deleted using methods designed to prevent recovery or reconstruction. These processes ensure that data is not retained unnecessarily and that storage risks are minimized.

NewEra also implements controls to ensure the integrity and accuracy of data. Measures are in place to prevent unauthorized modification, and systems are designed to maintain reliable and consistent records of transactions and activities. This is particularly critical in the context of gaming operations and financial transactions, where data integrity directly impacts fairness, accountability, and regulatory compliance.

Where data is processed or stored by third-party service providers, NewEra ensures that appropriate contractual and technical safeguards are in place to protect that data in accordance with the Company's standards. This includes requirements relating to data security, confidentiality, and incident reporting.

7. System and Network Security

NewEra maintains a comprehensive system and network security framework designed to protect its technology infrastructure against unauthorized access, disruption, or compromise. This framework is based on a layered security approach, combining preventive, detective, and responsive controls to ensure that risks are effectively mitigated across all environments in which the Company operates.

The Company's systems are deployed within controlled and secure environments, whether on dedicated infrastructure or through trusted cloud service providers. Network security controls are implemented to regulate and monitor traffic entering and leaving these environments. Firewalls, traffic filtering mechanisms, and other network protection technologies are used to restrict access to authorized sources and to prevent malicious activity from impacting critical systems.

All systems within the Company's environment are configured in accordance with secure configuration standards designed to minimize vulnerabilities. Default settings are reviewed and adjusted as necessary, unnecessary services are disabled, and system hardening practices are applied to reduce the attack surface. These configurations are maintained and reviewed periodically to ensure ongoing effectiveness.

Endpoint protection measures, including anti-malware and intrusion detection mechanisms, are implemented to safeguard servers, workstations, and other devices against malicious software and unauthorized activity. Systems are continuously monitored to detect potential threats, and alerts are generated where suspicious behavior is identified.

NewEra operates a structured vulnerability management process to identify and address security weaknesses in a timely manner. This includes regular vulnerability scanning, assessment of identified issues based on risk, and prompt application of security patches and updates. Critical

vulnerabilities are prioritized and remediated without undue delay to reduce exposure to exploitation.

Access to the Company's network and systems is tightly controlled and monitored. Secure protocols are enforced for all communications, and remote access is permitted only through controlled mechanisms that require strong authentication. Network segmentation is applied where appropriate to separate critical systems from less sensitive environments, thereby limiting the potential impact of a security breach.

The Company also implements protections against external threats such as distributed denial-of-service (DDoS) attacks, recognizing the importance of maintaining platform availability in an online gambling environment. Monitoring systems are designed to detect abnormal traffic patterns and trigger appropriate mitigation measures to preserve service continuity.

System activity, including access attempts, administrative actions, and network events, is logged and monitored to support the detection and investigation of potential security incidents. These logs are protected to ensure their integrity and are retained in accordance with the Company's logging and monitoring standards.

8. Change Management and Secure Development

NewEra maintains a structured and controlled approach to the management of changes across its systems, applications, and infrastructure in order to ensure the continued security, stability, and integrity of its operating environment. Recognizing that system changes represent a key source of potential risk, the Company has established processes that ensure all changes are properly assessed, authorized, tested, and implemented in a controlled manner.

All changes to production systems, including software updates, configuration modifications, infrastructure adjustments, and integrations with third-party services, are subject to a formal change management process. Changes are required to be documented in advance, with sufficient detail to describe the nature of the change, the systems affected, and the intended outcome. Each change is subject to review and approval by the appropriate team to ensure that it is justified, properly scoped, and aligned with business and security requirements.

As part of this process, the potential impact of each change on system security is assessed prior to implementation. This includes consideration of whether the change may introduce new vulnerabilities, affect existing controls, or alter access permissions or data flows. Where relevant, input is obtained from both the Tech Team and the Compliance Team to ensure that security and regulatory considerations are adequately addressed.

Testing is a mandatory component of the change process. Changes are first implemented in controlled, non-production environments, such as development or staging environments, where they are tested to confirm that they function as intended and do not introduce unintended risks or disruptions. Only after successful testing and formal approval are changes deployed to production systems.

For critical systems, including the gaming platform and payment processing systems, additional safeguards are applied. These may include enhanced testing, staged deployments, and increased monitoring during and after implementation to ensure that any issues are detected and addressed promptly. Where appropriate, rollback procedures are defined in advance to allow systems to be restored to a previous stable state in the event of failure or unexpected outcomes.

NewEra also integrates security considerations into its software development practices. Development activities are conducted with an awareness of secure coding principles, and efforts are made to ensure that applications are designed and implemented in a manner that minimizes exposure to common vulnerabilities. Where applicable, code reviews, vulnerability testing, and other assurance activities are performed prior to deployment.

All changes are logged and recorded, creating an auditable trail that supports oversight, accountability, and review. These records are retained and may be used to demonstrate compliance with internal policies and regulatory expectations.

9. Incident Management and Response

NewEra maintains a structured and coordinated approach to the identification, reporting, management, and resolution of information security incidents. The objective of this framework is to ensure that any event which may compromise the confidentiality, integrity, or availability of systems or data is addressed promptly, effectively, and in a manner that minimizes impact on operations, users, and regulatory compliance.

An information security incident is defined as any actual or suspected event that results in, or has the potential to result in, unauthorized access to systems or data, data loss or leakage, service disruption, fraud, or any breach of established security controls. This includes, but is not limited to, cyberattacks, account compromise, system intrusions, malware infections, denial-of-service attacks, and internal misuse of systems.

All personnel are required to report suspected or confirmed security incidents without delay through established internal reporting channels. Upon identification, incidents are formally recorded and assessed to determine their nature, scope, and potential impact. This initial

assessment enables appropriate prioritization and ensures that resources are allocated in line with the severity of the incident.

The Tech Team is responsible for the technical handling of incidents, including containment, investigation, and remediation. Immediate actions are taken to limit the spread or escalation of the incident, which may include isolating affected systems, restricting access, or suspending compromised accounts. At the same time, steps are taken to preserve relevant evidence to support investigation and analysis.

The Compliance Team oversees the incident management process to ensure that incidents are handled in accordance with internal procedures and regulatory expectations. This includes determining whether notification obligations apply and ensuring that relevant stakeholders are informed where necessary. The Management Team is kept informed of significant incidents, particularly those with material operational, financial, or reputational impact.

Following containment, a detailed investigation is conducted to identify the root cause of the incident, assess the extent of any impact, and determine whether any data or systems have been compromised. Based on these findings, appropriate remediation measures are implemented to restore affected systems and prevent recurrence. Recovery activities are performed in a controlled manner to ensure that systems are returned to a secure and stable state.

All incidents are documented comprehensively, including the timeline of events, actions taken, decisions made, and outcomes achieved. Post-incident reviews are conducted for significant events to evaluate the effectiveness of the response and to identify opportunities for improvement. Lessons learned are incorporated into the Company's security framework, including updates to controls, procedures, and training where necessary.

10. Business Continuity and Disaster Recovery

NewEra maintains a structured and proactive approach to business continuity and disaster recovery to ensure that its critical operations can continue, or be restored within an acceptable timeframe, in the event of a disruption. This framework is designed to minimize operational impact, protect data integrity, and maintain service availability for users, even under adverse conditions.

The Company recognizes that, as an online gambling operator, uninterrupted access to its platform and the integrity of player balances and transactional data are essential. Accordingly, continuity and recovery planning are focused on ensuring that critical systems, including the gaming platform, payment processing systems, and supporting infrastructure, are resilient and recoverable.

NewEra implements regular data backup procedures for all critical systems and data. Backups are performed at a frequency appropriate to the importance and sensitivity of the data, with particular emphasis on transactional records, player account balances, and operational databases. Backup data is stored securely, including in geographically separate or logically isolated environments where appropriate, to protect against data loss resulting from system failures, cyber incidents, or physical disruptions.

Backup processes are monitored to ensure successful completion, and records of backup activities are retained. In addition, restoration procedures are tested periodically to verify that data can be recovered accurately and within defined timeframes. These tests are designed to ensure that backup data is reliable and that recovery processes are effective in practice, rather than solely in theory.

NewEra maintains documented procedures for responding to major disruptions, including system outages, infrastructure failures, cyber incidents, or third-party service interruptions. These procedures define the steps required to restore systems and services, including prioritization of critical functions, allocation of responsibilities, and coordination between teams.

Recovery objectives are defined for key systems, including target timeframes for restoring operations and acceptable levels of data loss. These objectives guide the design of backup and recovery processes and ensure that recovery efforts are aligned with business priorities.

The Tech Team is responsible for executing backup and recovery procedures and for maintaining the technical capabilities required to support system restoration. The Compliance Team oversees the adequacy of continuity arrangements and ensures that they remain aligned with regulatory expectations. The Management Team is informed of significant disruptions and oversees the overall response to ensure that business impacts are appropriately managed.

Where NewEra relies on third-party service providers for critical infrastructure or services, the Company considers the resilience and recovery capabilities of those providers as part of its vendor management and risk assessment processes. This ensures that dependencies do not introduce unacceptable risks to business continuity.

11. Third-Party Security Management

NewEra recognizes that its reliance on third-party service providers introduces additional information security risks that must be effectively managed. These providers play a critical role in supporting the Company's operations, including areas such as platform infrastructure, hosting services, payment processing, identity verification, software development, and technical support.

As such, NewEra maintains a structured approach to ensuring that all third-party relationships are subject to appropriate security oversight and control.

Prior to engaging any third-party provider, NewEra conducts a due diligence process to assess the provider's suitability from both an operational and security perspective. This assessment considers the nature of the services provided, the level of access to Company systems or data, and the provider's ability to meet the Company's security and compliance requirements. Where relevant, this may include a review of the provider's security practices, certifications, policies, and historical performance.

Security requirements are formally established as part of the contractual arrangements with third-party providers. These requirements are designed to ensure that providers implement appropriate measures to protect NewEra data and systems, maintain confidentiality, and respond effectively to security incidents. Contracts may also include provisions relating to data protection, access control, incident notification, audit rights, and service availability.

NewEra ensures that access granted to third-party providers is limited to what is necessary for the performance of their services and is subject to the same access control principles applied internally. Such access is monitored and reviewed periodically to ensure it remains appropriate and does not introduce unnecessary risk.

The Company maintains ongoing oversight of its third-party relationships to ensure continued compliance with security expectations. This includes periodic reviews of provider performance, reassessment of associated risks, and monitoring of any changes in the provider's services or operating environment that may impact security. Where issues or deficiencies are identified, appropriate actions are taken to address them in a timely manner.

Third-party risks are incorporated into the Company's overall risk management framework, ensuring that dependencies are fully considered in the assessment of the Company's security posture. In the event of a security incident involving a third-party provider, NewEra coordinates its response in line with its incident management procedures, ensuring that impacts are contained and addressed effectively.

12. Security Awareness and Training

NewEra recognizes that effective information security depends not only on technical controls but also on the awareness, understanding, and behavior of its personnel. As such, the Company maintains an ongoing program to ensure that all individuals acting on its behalf are informed of their responsibilities and equipped to identify and respond to security risks in the course of their work.

All personnel are required to adhere to the Company's information security principles and to exercise due care when handling systems and data. This responsibility is supported through structured awareness and training initiatives designed to promote a consistent understanding of security requirements across the organization.

Security awareness is introduced as part of the onboarding process, ensuring that new personnel are informed of the Company's policies, acceptable use standards, and key security risks from the outset of their engagement. This includes guidance on the proper handling of sensitive information, secure use of systems, password and authentication practices, and the identification of common threats such as phishing and social engineering.

In addition to initial onboarding, NewEra provides periodic refresher training to reinforce key concepts and to address emerging threats. This ensures that personnel remain aware of evolving risks and are able to adapt their behavior accordingly. Training content is reviewed and updated as necessary to reflect changes in the threat landscape, internal systems, or regulatory expectations.

Personnel are expected to remain vigilant and to report any suspected security incidents, weaknesses, or unusual activities without delay. Clear reporting channels are established to support this process, and individuals are encouraged to raise concerns without hesitation. This proactive reporting culture supports early detection of potential issues and contributes to the overall effectiveness of the Company's security framework.

The Company also promotes acceptable use of its systems and resources, ensuring that these are used only for authorized purposes and in a manner that does not compromise security. Where appropriate, additional guidance may be provided for specific roles or functions that involve access to particularly sensitive systems or data.

Records of training and awareness activities are maintained to demonstrate compliance with this requirement and to support oversight by the Compliance Team. Participation in required training is monitored, and follow-up actions may be taken where necessary to ensure that all personnel meet the expected standards.

13. Monitoring, Logging, and Security Oversight

NewEra maintains comprehensive monitoring and logging mechanisms to support the ongoing protection of its systems, data, and operations. These mechanisms are designed to ensure that relevant activities are recorded, that potential security threats are detected in a timely manner, and that sufficient information is available to support investigation, audit, and regulatory requirements.

Logging is implemented across all critical systems and environments, including the gaming platform, payment processing systems, administrative tools, and underlying infrastructure. Events that are recorded include, but are not limited to, user access and authentication attempts, administrative actions, system changes, transaction activity, and security-related events. This approach ensures that a complete and traceable record of system activity is maintained.

Logs are generated and stored in a manner that preserves their accuracy and integrity. Appropriate safeguards are implemented to prevent unauthorized modification, deletion, or tampering with log data. Access to logs is restricted to authorized personnel, and segregation of duties is maintained to ensure that individuals with system administration privileges do not have unrestricted ability to alter audit records.

NewEra retains log data for a period consistent with operational, legal, and regulatory requirements. Retention periods are defined to ensure that logs remain available for the purposes of investigation, dispute resolution, and compliance verification, particularly in relation to player activity and financial transactions.

Monitoring processes are applied to log data to identify unusual, suspicious, or unauthorized activities. These processes may include automated alerting mechanisms, as well as periodic manual reviews conducted by the Tech Team and, where appropriate, the Compliance Team. The frequency and depth of log reviews are determined based on the criticality of the systems involved and the associated level of risk.

Where anomalies or potential security events are identified through monitoring activities, they are investigated in accordance with the Company's incident management procedures. This ensures that any issues are assessed, escalated where necessary, and addressed in a timely and controlled manner.

Monitoring also supports the broader oversight of system performance and security posture. By maintaining visibility over system activity and trends, NewEra is able to identify potential weaknesses, improve controls, and respond proactively to emerging risks.

14. Policy Review and Continuous Improvement

NewEra is committed to ensuring that its Information Security Policy remains effective, relevant, and aligned with the Company's operational environment, risk profile, and regulatory obligations. To support this objective, the Policy is subject to a structured review and continuous improvement process designed to ensure that it evolves in response to internal developments and external changes.

This Policy is formally reviewed at least on an annual basis to assess its adequacy and effectiveness. The review considers a range of factors, including changes in the Company's systems, infrastructure, or business model; the introduction of new technologies or third-party providers; developments in the threat landscape; and updates to applicable legal, regulatory, or licensing requirements.

In addition to scheduled reviews, this Policy is also subject to ad hoc updates where necessary. Such updates may be triggered by significant information security incidents, identification of control weaknesses, audit findings, or material changes in operational processes. This ensures that the Policy remains responsive and continues to provide appropriate guidance under changing conditions.

The Compliance Team is responsible for coordinating the review process, including gathering input from relevant teams, assessing the effectiveness of existing controls, and identifying areas where enhancements may be required. The Tech Team contributes to this process by providing insight into system changes, technical risks, and the performance of security controls in practice. The outcomes of the review are documented and submitted to the Management Team for consideration.

The Management Team is responsible for approving any updates to this Policy and ensuring that changes are implemented appropriately across the organization. Where updates are made, the revised Policy is communicated to relevant personnel to ensure continued awareness and compliance.

Version control is maintained to ensure that all changes to the Policy are properly documented. This includes maintaining a record of revisions, approval dates, and a summary of key changes. Such records support transparency, auditability, and regulatory review.

As part of its commitment to continuous improvement, NewEra also considers feedback from internal monitoring activities, incident reviews, and external assessments, including audits or regulatory interactions. Lessons learned from these sources are incorporated into the Policy and related procedures to strengthen the Company's overall security posture.

15. Compliance and Enforcement

Compliance with this Information Security Policy is mandatory for all personnel and third parties operating on behalf of NewEra. The Company requires that all individuals and entities within the scope of this Policy adhere strictly to its principles, controls, and associated procedures in order to maintain a secure and compliant operating environment.

NewEra maintains oversight mechanisms to monitor adherence to this Policy and to ensure that information security controls are implemented and operating effectively. This includes internal reviews, monitoring activities, and, where applicable, audits conducted either internally or by external parties. These activities are designed to assess compliance, identify potential weaknesses, and support the ongoing improvement of the Company's information security framework.

All personnel are expected to understand their responsibilities under this Policy and to conduct their activities in a manner that supports the protection of NewEra's systems and data. Failure to comply with the requirements set out in this Policy may result in disciplinary action, up to and including termination of employment or contractual arrangements, depending on the nature and severity of the breach.

Where non-compliance is identified, NewEra will take appropriate corrective action to address the issue and to prevent recurrence. This may include remediation of control weaknesses, updates to procedures, additional training, or changes to access rights. In cases where non-compliance results in a security incident or regulatory concern, escalation procedures will be followed in accordance with the Company's incident management and governance frameworks.

Third-party providers are also required to comply with applicable security requirements as defined in contractual agreements. Failure by a third party to meet these obligations may result in remedial action, including restriction of access, suspension of services, or termination of the relationship, depending on the severity of the issue.

NewEra is committed to maintaining compliance with all applicable legal, regulatory, and licensing requirements relating to information security and data protection. Where required, the Company will cooperate with regulatory authorities and provide evidence of its security controls, policies, and practices.

Through the consistent enforcement of this Policy, NewEra ensures that information security is upheld as a fundamental requirement across all aspects of its operations, supporting both regulatory compliance and the protection of its business, systems, and stakeholders.