Process for Non-Compliance

This is the KLERQ Process for Non-Compliance, relevant for those wishing to create an account and utilize the services provided by KLERQ.

This Process for Non-Compliance is in Version 1.1, with the latest revision dated *August 21, 2024*

Ensuring compliance with organizational policies, including cybersecurity, data protection, and general conduct, is vital to maintaining the integrity and security of our operations. The Disciplinary Process for Non-Compliance outlines the procedures for addressing violations of these policies. This process ensures that all instances of non-compliance are handled fairly, consistently, and transparently.

Section 1: Scope

This process applies to all employees, contractors, temporary staff, and any other individuals who have a formal relationship with the organization and are subject to its policies and procedures.

(a) Objectives:

i) To address non-compliance in a manner that is fair and consistent.
ii) To correct behavior and prevent future violations.
iii) To protect the organization's assets and reputation.
iv) To ensure compliance with legal and regulatory requirements.

(b) Identification of Non-Compliance
Non-compliance may be identified through various means, including but not limited to:

i) Routine audits and inspections
ii) Monitoring and surveillance systems
iii) Reports from employees or third parties
iv) Incident reports and investigations

(c) Reporting Non-Compliance

i) Any individual who identifies a potential non-compliance issue should report it promptly to their supervisor, the Compliance Officer, or through the organization's anonymous reporting channel.
ii) Reports should include a detailed description of the non-compliance, evidence if available, and the names of involved parties.

(d) Initial Investigation

i) Preliminary Assessment

The Compliance Officer or designated investigator will conduct a preliminary assessment to determine if the reported non-compliance warrants a formal investigation. This assessment includes reviewing the initial report, gathering preliminary evidence, and interviewing relevant parties.

ii) Investigation

If a formal investigation is warranted, a thorough examination of the facts will be conducted. This includes collecting evidence, interviewing witnesses, and documenting findings. Investigations will be conducted impartially and confidentially to ensure fairness and protect the privacy of all individuals involved.

(e) Notification and Response

i) Notification

Individuals involved in the investigation will be notified of the alleged non-compliance and given an opportunity to respond. Notification should include:

a. A summary of the allegations
b. Details of the evidence gathered
c. Information about the investigation process

ii) Response

a. The individual(s) will be given a reasonable period to provide their response or defense. This may include written statements, evidence, or interviews.

(f) Determination of Disciplinary Action

i) Decision-Making

a. Following the investigation, a disciplinary decision will be made based on the severity of the non-compliance, the evidence presented, and any mitigating or aggravating factors.
b. The decision-making authority, such as the Disciplinary Committee or HR Manager, will review all findings and recommend appropriate disciplinary action.

ii) Disciplinary Actions

a. Verbal Warning: For minor or first-time offenses, a verbal warning will be issued. The nature of the violation and expectations for future behavior will be discussed.
b. Written Warning: For repeated or more serious violations, a formal written warning will be issued. This document will outline the nature of the non-compliance, required corrective actions, and potential consequences of further violations.
c. Suspension: In cases of significant non-compliance, a temporary suspension may be enforced. This action will be documented, and the individual will be informed of the suspension period and conditions for return.
d. Termination: For severe or repeated violations that impact organizational security or operations, termination of employment or contract may be considered. This decision will be made in accordance with legal and organizational guidelines.

(g) Appeal Process

i) Right to Appeal

a. Individuals who receive disciplinary action have the right to appeal the decision. The appeal process ensures that individuals have an opportunity to contest the decision if they believe it is unjust.

ii) Appeal Submission

a. Appeals must be submitted in writing within a specified timeframe (e.g., 10 business days) from the date of the disciplinary decision. The appeal should include a detailed explanation of the grounds for contesting the decision.

iii) Appeal Review

a. An appeal review committee, independent of the initial decision-makers, will review the appeal. This committee will assess the validity of the appeal and make a final decision.
b. The outcome of the appeal will be communicated in writing, including any changes to the original disciplinary action.

(h) Documentation and Reporting

i) Documentation

a. All steps of the disciplinary process, including investigations, actions taken, and appeals, must be thoroughly documented.
b. Documentation should include all relevant evidence, correspondence, and decisions. This information must be stored securely and accessible only to authorized personnel.

ii) Reporting

a. Summary reports of disciplinary actions will be reviewed periodically to ensure compliance with organizational policies and identify areas for improvement.
b. The reports should be reviewed by senior management to ensure consistency and fairness in the application of disciplinary actions.

(i) Training and Awareness

i) Employee Training

a. Employees and contractors will receive training on the organization's policies and the disciplinary process. This training will cover expectations for behavior, compliance requirements, and the procedures for reporting and addressing non-compliance.

ii) Ongoing Communication

a. Regular reminders about compliance expectations and the consequences of non-compliance will be communicated through internal channels, such as newsletters, meetings, and updates to the employee handbook.

(j) Review and Improvement

i) Process Review

a. The disciplinary process will be reviewed annually to ensure its effectiveness and alignment with best practices. Feedback from employees, managers, and other stakeholders will be considered during this review.

ii) Process Improvement
   a. Updates to the disciplinary process will be made as necessary based on the review findings and any changes in legal or regulatory requirements.
   b. All changes to the process will be communicated to relevant parties, and updated documentation will be distributed as needed.

(k) Conclusion

Maintaining a disciplined and compliant organizational environment is essential for protecting the organization's assets, reputation, and operational effectiveness. This Disciplinary Process for Non-Compliance provides a structured framework for addressing violations in a fair and consistent manner.

Section 2: Scope and Applicability

2.1. Covered Systems and Data:

This cybersecurity policy applies to all information systems, data, and technology resources owned, operated, or managed by KLERQ, including but not limited to:

KLERQ's Software as a Service (SaaS) platform, which includes information pertaining to law firms.
Hosting services provided by Microsoft Azure, where KLERQ's SaaS platform is hosted.
The policy encompasses various categories of data, including but not limited to:

i) Matter information
ii) Referees (contact details)
iii) Personal information about lawyers (name phone numbers, email addresses, photos)
iv) Commercial text related to practices, focus industries and the firm in general
v) Publications
vi) Quotes
vii) Information about pitches
viii) Information for submissions documents

2.2. Personnel:

This policy is applicable to all divisions and departments within KLERQ, including but not limited to:

i) Technology
ii) Sales
iii) Marketing
iv) Support
v) Customer Success

Additionally, this policy extends to law firms and external entities with whom KLERQ collaborates, including:

vi) Microsoft Azure (as the cloud provider)
vii) External development agency Stijlbreuk
viii) All employees, contractors, temporary workers, and third-party vendors within these divisions and entities who have access to KLERQ's systems and data are required to comply with this policy.

2.3. Policy Review and Updates:

This cybersecurity policy will undergo regular reviews, at a minimum, once every half a year. Additional reviews will be conducted in the event of major changes to the software, the engagement of new sub-vendors, or significant shifts in technology or regulations. Updates to the policy will be made to address emerging threats, ensure compliance, and maintain the highest standards of data security.

Section 3: Roles and responsibilities

3.1 Key Personnel and Roles:

i) KLERQ (Internal)
• Technology Department: Manages day-to-day technology operations, including system security, access control, and incident response.
o Contact: Tim Strijbosch (Head of Technology)
• Sales and Marketing Team: Ensures that client interactions align with security policies and guidelines.
o Contact: Stijn van Oirschot (Head of Sales and Marketing)
• Management Team: Provides executive oversight and guidance for cybersecurity practices.
o Contact: Jorn Vermeulen (Director)
• Support Team: Assists clients with security-related inquiries and reports incidents as necessary.
• Administration Team: Supports cybersecurity efforts through policy enforcement and employee training.
• Customer Success Team: Collaborates with clients to address security concerns and promote cybersecurity awareness.

ii) External:
• Microsoft Azure (External Cloud Provider)
o Azure Security Team: Manages the security of the cloud infrastructure and ensures physical and network security within Azure data centers.
o Azure Support Team: Provides assistance in addressing security-related concerns within the Azure environment.
• Stijlbreuk (External Development Agency)
o Development Team: Collaborates with KLERQ on software development, ensuring that security best practices are followed and vulnerabilities are promptly addressed.
o Incident Response Contact: Designated point of contact at Stijlbreuk for reporting and addressing security incidents related to software development.

3.2 Reporting Structure:

The main points of contact for cybersecurity and incident management within KLERQ are:

i) Tim Strijbosch (Head of Tech)
ii) Stijn van Oirschot (Head of Sales and Marketing)
iii) Jorn Vermeulen (Director)

They can be reached via the dedicated email address: security@klerq.io . This email address serves as the primary channel for reporting security incidents and related concerns within KLERQ.

3.3 Policy Review and Updates:

To ensure the effectiveness of this cybersecurity policy, it will be reviewed at least once every half a year. Additionally, reviews will occur in response to significant changes to the software, engagement

of new sub-vendors, or substantial shifts in technology or regulations. Updates to the policy will be made to address emerging threats, ensure compliance, and maintain the highest standards of data security.

Section 4: Information Classification

4.1. Categories of Information:

KLERQ handles various categories of information, including but not limited to:

i) Personal Information: Data related to individuals, including clients and employees.
ii) Company Information: Information about organizations and businesses.
iii) Commercial Information: Data related to commercial practices, focus industries, and client interactions.

4.2. Data Classification Labels:

By default, all customer information is classified as "Confidential." This classification applies to all information concerning clients, whether within or outside KLERQ's tooling, and includes information shared during customer support interactions.

Within the KLERQ tooling, clients have the option to label specific information as "Confidential" or "Publishable." However, these labels do not alter the overall classification or handling of the information.

4.3. Handling and Protection:

i) Encryption: All information within the KLERQ system, including data received for implementations (e.g., submissions, pitches, referee lists), is encrypted using SSL (Secure Sockets Layer) throughout the entire platform.
ii) Need-to-Know Basis: Access to information is granted based on the principle of "need-to-know." Only authorized individuals within specific roles are granted access to information as required for their responsibilities.
iii) Access Control: Access to customer information is controlled and limited to the following roles:
iv) Technology: Access to implementation documentation received from clients, strictly for the required period, governed by NDAs.
v) Customer Success: Access for onboarding purposes, limited to the information necessary for their tasks.
vi) Support: Access is enabled by the client and is only provided in response to client inquiries.
vii) Sales: Access to client data for demonstration purposes, as specified by the client.
viii) Other Categories: No default access to customer information.

4.4. Data Labeling:

Data within the KLERQ system is labeled as "Confidential" by default, with the option for clients to label specific information as "Confidential" or "Publishable" within the tooling.

4.5. Data Handling Procedures:

i) Support Data: Support data is retained for a maximum of 30 days after the ticket is successfully resolved.
ii) Customer Success Data: Customer Success works in conjunction with the Technology Department for implementation and retains information for 30 days after successful implementation. During this period, data is stored in an extra-protected Microsoft cloud

environment, accessible only to the implementation and tech teams. Information may also be securely transmitted to KLERQ via protected environments.

Section 5: Access Control

5.1. Roles and Departments:
Access control is defined based on specific roles and departments within KLERQ. The following roles and departments have access to various categories of information:

i) Technology: Responsible for system management.
ii) Sales: Engages with client data on request.
iii) Customer Success: Manages client relationships and implementations.
iv) Support: Assists clients with technical inquiries.

5.2. Data Access Permissions:
Access permissions for each role are as follows:

i) Technology: View, delete, and transfer client data.
ii) Sales: View client data (access granted upon client request).
iii) Customer Success: View, edit, delete, and transfer client data (access granted upon client request).
iv) Support: View and edit client data (access granted upon client request).

5.3. Conditions for Access:

Access is granted based on the specific responsibilities and requirements of each role. For Sales, Customer Success, and Support, access is granted upon client request, ensuring that clients have control over their data access.

5.4. Access Revocation:

Access is regularly reviewed and checked by the Technology team on a monthly basis. An access control scheme is maintained to track who has access to which client data and for what period. Access is revoked as part of the offboarding process when it is no longer required.

5.5. Monitoring and Auditing:

Access to information is continuously monitored and audited to ensure compliance with this policy. Audit logs are maintained to track access activities.

5.6. Reporting and Accountability:

Incidents or breaches related to access control should be reported through the established incident management process. Accountability for proper access management lies with the respective roles and departments responsible for data access.

5.7. Security Checks:

KLERQ undergoes annual penetration testing to assess and enhance its security posture. Regular security checks are conducted in collaboration with the external development team. Access to an external security advisor is maintained to ensure ongoing security vigilance and best practices.

Section 6: Incident Management

6.1. Incident Response Team:

The incident response team at KLERQ consists of the following key personnel:

i) Director: Jorn Vermeulen

ii) Head of Sales and Marketing: Stijn van Oirschot
iii) Head of Technology: Tim Strijbosch

6.2. Incident Categories:

Cybersecurity incidents at KLERQ are categorized into the following types, among others:

i) Data breaches
ii) Malware infections
iii) Unauthorized access
iv) Denial of service attacks
v) Other incidents impacting data security

6.3. Incident Reporting:

Employees, clients, or other stakeholders should promptly report cybersecurity incidents to the designated incident response team via the following channels:
Email: security@klerq.io
Phone: +31 085 060 60 24 (During business hours)

6.4. Incident Assessment:

Upon receiving a report of a cybersecurity incident, the incident response team, in conjunction with the client and KLERQ's external technology partner, will assess and categorize the incident's severity based on predefined criteria.

6.5. Response Procedures:

The incident response procedures include the following steps:

i) Containment: Isolate affected systems to prevent further damage.
ii) Eradication: Remove the threat and vulnerabilities causing the incident.
iii) Recovery: Restore affected systems and services to normal operation.
iv) Lessons Learned: Review the incident to identify areas for improvement.

6.6. Communication:

Incident information will be communicated as follows:

i) Internally: The incident response team will coordinate internal communication.
ii) Externally: Clients will be informed within 24 hours for major incidents and within 5 business days for minor incidents. Minor incidents are those with no significant impact.

6.7. Documentation:

All cybersecurity incidents will be documented, and the incident report will include the following structure:

i) Incident details and description
ii) Incident category and severity
iii) Actions taken during incident response
iv) Impact assessment
v) Recommendations for prevention

6.8. Review and Improvement:

Incidents will be reviewed after resolution to identify areas for improvement in incident response procedures and overall cybersecurity. This review process includes annual security meetings with clients to discuss relevant topics.

Section 7: Training and Awareness

7.1. Training Requirements:

i) All employees receive comprehensive data security training during their onboarding process.
ii) Data security is a recurring topic in monthly company meetings.
iii) Quarterly security updates and training sessions are conducted, led by external specialists and/or the Head of Technology. These sessions may include participation from the external development agency.

7.2. Training Delivery:

Whenever possible, cybersecurity training is conducted in person to facilitate effective learning and engagement.

7.3. Awareness Programs:

i) Employees are encouraged to support each other in maintaining a culture of cybersecurity awareness.
ii) Specific topics, such as password protection and secure data handling and storage, are addressed through internal one-pagers.
iii) Periodic checks are conducted to assess and reinforce cybersecurity practices.

7.4. Roles and Responsibilities:

i) Head of Technology: Oversees all internal security processes and serves as the main point of contact for internal security matters.
ii) Head of Sales: Responsible for all customer-related communications regarding security.
iii) Director: Holds overall responsibility for the cybersecurity process.

7.5. Reporting and Compliance:
Cybersecurity training and awareness compliance are monitored and reported.

7.6. Documentation:
Training documentation is utilized during the onboarding process and is centrally accessible to all employees for ongoing reference and improvement. Information is reviewed and updated quarterly to ensure relevance and effectiveness.

Section 8: Access Control

8.1. Access Control Policy:

KLERQ's access control policy is founded on the principle of granting individuals access only to the resources they need to perform their roles effectively and securely. The policy aims to maintain the confidentiality, integrity, and availability of data and systems.

8.2. Access Rights:

Access rights are assigned based on the principle of least privilege. Employees and authorized individuals receive access rights customized to their roles and specific needs within the organization. Criteria for determining access include job responsibilities and tasks.

8.3. Access Control Mechanisms:

Authentication: Access control is enforced through strong authentication methods, including username and password or multi-factor authentication (MFA).

Role-Based Access Control (RBAC): Customized roles are created to ensure that individuals have access only to the functions and data necessary for their roles.

Password Manager: A strong password manager is utilized to ensure password complexity, expiration, and secure storage.

8.4. Password Policies:

Password Complexity: Passwords must meet complexity requirements, including length, character types, and regular updates.

Password Manager: A password manager is recommended to generate, store, and manage complex passwords securely.

8.5. Multi-Factor Authentication (MFA):

MFA is implemented and available upon request for clients using Microsoft Azure services, enhancing the security of user authentication.

8.6. User Account Management:

User accounts are created, modified, and deactivated by administrators based on the needs of employees and the organization. Terminated employees' access rights are promptly revoked.

8.7. Remote Access:

Secure Connections: Remote access is secured through the use of Virtual Private Network (VPN) connections, ensuring encrypted data transmission.
Authentication: Strong authentication methods are employed for remote access.

8.8. Access Review and Auditing:

Access rights are subject to periodic review to ensure alignment with job roles and responsibilities.

Auditing of user access and changes to access rights is conducted regularly to detect and respond to unauthorized access.

8.9. Incident Response:

Access control is integrated into the incident response process to promptly address unauthorized access or security breaches. Measures are in place to investigate, contain, and mitigate any incidents related to access control.

Section 9: Backup and Recovery

9.1. Backup Policy:

KLERQ's backup and recovery policy aim to ensure the availability and integrity of data. Key objectives include data protection, minimizing data loss, and rapid recovery in the event of data loss or system disruptions.

9.2. Data Backup Procedures:

Data is backed up every hour using Microsoft Azure services.
Primary backup copies are stored in The Netherlands, ensuring data redundancy and availability.

Additional fallback backup copies are securely maintained in an EER (European Economic Area) country to further safeguard against data loss.

9.3. Retention Period:

Backup data is retained for a period of 30 days, providing a comprehensive data recovery window.

9.4. Data Recovery Procedures:

Data recovery procedures are managed jointly by the Technology department and our external development partner.

In the event of data loss or system disruptions, the responsible teams initiate the recovery process promptly to minimize downtime.

Data recovery is designed to be efficient, ensuring that data can be restored quickly.

9.5. Testing and Verification:

Backups are regularly tested and verified to ensure their integrity and reliability. This includes conducting test restores to confirm data recoverability.

9.6. Backup Encryption:

Azure Backup automatically encrypts all backed-up data using 256-bit AES encryption while storing it in the Azure cloud. This encryption ensures the security and compliance of stored data.

9.7. Off-Site Storage:

Primary and fallback backup copies are securely maintained, providing redundancy and disaster recovery capabilities. Off-site storage in an EER country enhances data protection and availability.

9.8. Incident Response:

Backup and recovery procedures are integrated into the incident response process to address data loss or system disruptions promptly. Refer to Section 6 for details on the incident response process.

9.9. Business Continuity and Disaster Recovery (BCDR):

Azure Site Recovery (ASR) is utilized to implement a robust business continuity and disaster recovery (BCDR) strategy. ASR helps secure data, applications, and workloads during planned or unplanned outages, ensuring business continuity.

Section 10: Security Monitoring and Logging

10.1. Monitoring and Logging Policy:

KLERQ's security monitoring and logging policy are designed to proactively identify and respond to security threats, ensuring the confidentiality, integrity, and availability of our systems and data. The key objectives include early threat detection, incident response readiness, and continuous security improvement.

10.2. Monitoring Systems:

While we do not utilize a dedicated Security Information and Event Management (SIEM) system, we rely on regular log checks of our systems and leverage Azure logs to monitor our network, systems, and applications for potential security threats.

10.3. Event and Log Collection:

Security events and logs are collected from various systems, including servers, network devices, and cloud services, to provide comprehensive visibility into our environment.

10.4. Log Retention:

Security logs are retained for a minimum period of 90 days to support incident investigations and compliance requirements. Longer retention periods may be applied based on legal or regulatory obligations.

10.5. Log Analysis:

Our security team regularly analyzes security logs to identify anomalies, potential security incidents, and emerging threats. Automated and manual analysis techniques are employed to ensure thorough scrutiny.

10.6. Alerting and Notification:

Real-time alerts and notifications are generated when security incidents or anomalies are detected.

Alerts are delivered to designated security personnel, including the Director and Head of Technology, for immediate response.

10.7. Incident Response Integration:

Security monitoring and logging are tightly integrated into our incident response process (see Section 6). When security incidents are identified, incident response procedures are promptly initiated to contain and mitigate potential threats.

10.8. Regular Review and Reporting:

Security logs are subject to regular review to identify trends, potential weaknesses, and areas for improvement. Reports summarizing the results of log analysis are presented to the management team during security meetings.

Section 11: Change Management Process

To ensure the continued integrity, availability, and confidentiality of our information systems, all changes to the organization's technology infrastructure, applications, and services must follow a formal Change Management Process. This process helps to mitigate the risks associated with implementing changes.

11. 1 Scope: This process applies to all changes to systems, applications, network configurations, and other critical IT infrastructure components that could impact cybersecurity.

11. 2 Procedures:

i) Request for Change (RFC):
   a. All changes must begin with a documented Request for Change (RFC). This document must include the purpose, scope, impact analysis, and rollback procedures.
   b. The RFC must be submitted to the Change Advisory Board (CAB) for review.

ii) Impact Assessment:
   a. An impact analysis must be performed to understand the potential effects of the change on security, compliance, and business operations.
   b. Risk assessments should be conducted to identify any new vulnerabilities introduced by the change.

iii) Approval Process:
   a. The CAB, composed of representatives from IT, security, and relevant business units, will review the RFC.
   b. Only changes that have been fully assessed and deemed low-risk will be approved. High-risk changes may require additional controls or mitigation measures before approval.

iv) Implementation:
   a. Approved changes should be implemented following the documented plan, including any necessary security controls.
   b. All changes must be logged, and sufficient documentation must be maintained.

v) Post-Implementation Review:
   i. A review must be conducted after the change is implemented to ensure it has been successful and has not introduced any unexpected issues.
   ii. Lessons learned should be documented to improve future change management practices.

11. 3 Documentation:

i) All related documentation, including RFCs, impact assessments, and approvals, must be stored securely and be accessible for audit and review purposes.

12. User Access Rights Review Procedure

Managing user access to systems and data is a critical aspect of our cybersecurity strategy. To ensure that access rights are appropriate and secure, a formal User Access Rights Review Procedure has been established.

12. 1 Scope: This procedure applies to all employees, contractors, and third parties with access to the organization's systems and data.

12.2 Procedures:

i) Initial Access Provisioning:
   a. Access rights must be granted based on the principle of least privilege, ensuring users only have access to the data and systems necessary for their role.
   b. All access provisioning must be documented, including the justification for access and approval by the appropriate authority.

ii) Regular Access Reviews:
   a. User access rights must be reviewed on a quarterly basis to ensure they remain appropriate to the user's role.
   b. Reviews should include an audit of current access levels and verification with department heads to confirm the necessity of each access.

iii) Access Revocation:
   a. Access rights must be immediately revoked or adjusted when an employee changes roles, leaves the company, or no longer requires certain access.
   b. This process must be documented, and confirmation of revocation should be logged.

iv) Reporting and Documentation:
   a. All access review activities, including findings and actions taken, must be documented.
   b. Reports should be maintained for audit purposes and reviewed by the IT security team to ensure compliance with access management policies.

13. Visitor Log and Identification Procedure

To maintain the security of our physical premises and protect sensitive information, a formal procedure for logging and identifying all visitors has been implemented. This procedure ensures that only authorized individuals gain access to our facilities and that their presence is recorded.

13.1 Scope: This procedure applies to all visitors entering the premises, including contractors, delivery personnel, and guests.

13.2 Procedures:

i) Visitor Logging:
   a. All visitors must sign in at the reception desk upon arrival. The log must include the visitor's name, the purpose of their visit, the time of entry, and the person they are visiting.
   b. Visitors must sign out when leaving, with the time of departure recorded.

ii) Visitor Identification:
   a. Visitors are required to present official identification upon arrival. This ID will be checked against the visitor log to ensure accuracy.
   b. Visitors will be issued a temporary visitor badge, which must be worn visibly at all times while on the premises.

iii) Access Control:
   a. Visitors must be escorted by an employee at all times while within secure areas of the building.
   b. Access to restricted areas is not permitted unless expressly authorized and accompanied by a security staff member or relevant department head.

iv) Monitoring and Review:
   a. The visitor log will be reviewed regularly to ensure compliance with the procedure.
   b. Any discrepancies or security incidents involving visitors must be reported immediately to the security team.

v) Retention of Logs:
   a. Visitor logs will be retained for a minimum of six months and will be available for review by the security team or management upon request.

Section 14: Review and Revision

14.1. Policy Review Frequency:

This cybersecurity policy will be subject to regular review and updates to ensure its ongoing effectiveness. The policy will be reviewed at least once every six months by the security team and management to align with evolving cybersecurity threats, regulatory changes, and organizational needs.

14.2. Incident Management Testing:

Incident management procedures will be rigorously tested and evaluated on an annual basis or as needed in response to significant changes in the organization's technology environment, threat landscape, or incident response capabilities. Testing and revision will ensure that the incident management procedures remain effective and in sync with emerging threats.

Section 15: Conclusion

15.1. Commitment to Cybersecurity:

At KLERQ, we are unwavering in our commitment to safeguarding the confidentiality, integrity, and availability of data. This cybersecurity policy serves as a foundational framework to protect our

organization, our clients, and the sensitive information we handle. It reflects our dedication to maintaining the highest standards of cybersecurity and our continuous efforts to adapt to the ever-evolving threat landscape.

15.2. Employee Awareness:

We encourage all employees to familiarize themselves with this cybersecurity policy and the related incident management procedures. By understanding and adhering to these guidelines, each member of our organization plays a crucial role in upholding our cybersecurity practices and contributing to the protection of our data and our clients' data.

Section 16: Document Information

Classification	External use – selected clients (GDPR)
Reference	Internal Audit Procedure
Status	FINAL
Date	December 30, 2024
Owner	KLERQ
Approved by	Gerard Wentink

Version	**Date**	**Author**	**Summary of Changes**
1.1	21-Aug-2024	Stijn van Oirschot	Initial policy release;