kariera.group

Security White Paper

Security Classification: Public

Table of Contents

1 Introduction 3

2 Organization Security 3

2.1 Security Governance 3

2.2 Security Culture 3

2.3 Acceptable Use of Information 4

3 Product & Service Security 4

3.1 Secure Development Practices 4

3.2 Protection of Customer Data 4

3.3 Responsible Partner Ecosystem 4

3.4 Access Management 4

3.5 Monitoring & Oversight 5

3.6 Continuity & Resilience 5

4 Assurance & Assessments 5

4.1 Risk Management 5

4.2 Independent Reviews & Testing 5

4.3 Internal Audits 6

4.4 Continuous Improvement 6

5 Incident Management 6

6 Compliance 7

6.1 ISO/IEC 27001:2022 Alignment 7

6.2 GDPR Compliance 7

6.3 Supplier Management 7

7. Conclusion 7

1 Introduction

Kariera Group provides modern job board and HR technology solutions that support thousands of employers and candidates daily. Protecting the sensitive data flowing through our recruitment ecosystem is fundamental to our operations and core mission.

Our cybersecurity program is built upon industry-recognized standards and best practices, including ISO/IEC 27001:2022 and GDPR.

Through proactive risk management, secure engineering practices, and strong governance, we ensure the confidentiality, integrity, and availability of all systems and data across the Kariera Group.

Driven by a commitment to responsible data protection and continuous improvement, we consistently strengthen the security of our platform.

Our goal is simple: to give you confidence that your data is handled with care, enabling you to focus on finding the right people and supporting your organization's growth.

2 Organization Security

2.1 Security Governance

Kariera Group operates under a structured Security Governance Framework overseen by the Information Security Committee. This framework ensures ongoing oversight of security practices, risk management, and compliance obligations across the organization.

Our governance aligns with the:

- **ISO/IEC 27001:2022 international information security standard**
- **EU General Data Protection Regulation (GDPR)**
- **Applicable national data protection and cybersecurity laws**

Our Management Team is fully committed to establishing, implementing, and continuously improving our Information Security Management System (ISMS).

This commitment is demonstrated through:

- Allocation of adequate resources for information security and data protection.
- Clear definition of roles and responsibilities.
- Support for training and awareness initiatives.
- Regular review of security objectives and performance.

2.2 Security Culture

We maintain a strong security-oriented culture where employees understand their role in protecting information. Regular training, awareness programs, and ongoing communication help ensure that

staff can identify threats, follow secure practices, and uphold the organization's security and privacy policies.

2.3 Acceptable Use of Information

All employees are required to comply with clearly defined Acceptable Use guidelines that govern the proper and ethical use of information and technology resources.

These guidelines support confidentiality, ethical conduct, and compliance with the applicable security and privacy legal and contractual requirements.

3 Product & Service Security

3.1 Secure Development Practices

Security is embedded throughout the entire product and service development lifecycle. All new features undergo structured security reviews, risk assessments, and validation against established security principles before deployment.

This approach ensures that security considerations are addressed from design to release.

3.2 Protection of Customer Data

Kariera Group ensures that customer and candidate data is managed responsibly throughout its lifecycle, from collection and storage to processing and deletion.

We proactively identify and assess risks to data subjects, ensuring that appropriate measures are implemented to minimize potential impacts on their rights and freedoms.

To this end, we apply appropriate measures that protect privacy, enforce access controls, and ensure compliance with applicable legal, regulatory and contractual requirements.

3.3 Responsible Partner Ecosystem

We maintain a trusted partner ecosystem where all third-party providers are expected to meet security and privacy standards consistent with those upheld by Kariera Group.

Each partner undergoes a structured assessment and ongoing monitoring process to ensure that any information shared with them remains protected and handled responsibly throughout the engagement.

3.4 Access Management

Access to information and systems is carefully managed according to strict access control principles, ensuring that everyone is granted only the level of access required for their role.

This least-privilege and need-to-know approach helps protect sensitive information and promotes secure, responsible use across the organization.

To further strengthen this approach, Kariera Group uses Two-Factor Authentication (2FA) for key systems and services. This added verification layer provides stronger protection against unauthorized access and helps ensure that only verified users can access critical areas of the platform.

3.5 Monitoring & Oversight

Kariera Group maintains continuous oversight of its environment to identify irregularities or activities that may require attention. This proactive approach enables early detection and timely investigation of potential issues, helping ensure prompt response and minimizing impact on the security and reliability of our services.

3.6 Continuity & Resilience

Our business continuity and disaster recovery plans are designed to ensure the uninterrupted availability of our services, even in the event of operational disruptions.

These plans are regularly reviewed, updated, and tested to validate their effectiveness and ensure organizational readiness.

This approach enables Kariera Group to maintain resilient operations and quickly restore services when needed.

4 Assurance & Assessments

4.1 Risk Management

Risk management at Kariera Group is a continuous and proactive process. We regularly assess information security and data protection risks to ensure our security controls remain effective and appropriate.

As new threats or challenges arise, we adapt our measures accordingly to maintain strong protection across our services.

4.2 Independent Reviews & Testing

To validate the effectiveness and resilience of our security measures, we conduct several independent assessments performed by both internal experts and trusted third parties, including:

4.2.1 Penetration Testing

Periodic penetration tests performed by specialized external firms help us validate the resilience of our systems and identify areas for improvement. These assessments provide independent assurance and support continuous enhancement of our security posture.

4.2.2 Vulnerability Scanning

We perform regular automated vulnerability scans to detect weaknesses that may emerge over time. All findings are reviewed, prioritized, and remediated through our established risk management and remediation processes.

4.2.3 Threat Intelligence

Kariera Group leverages reputable threat intelligence sources to stay informed about emerging risks, industry trends, and evolving threat landscapes. This insight enables proactive decision-making and enhances our preparedness against potential threats.

4.3 Internal Audits

Internal audits are conducted by independent parties to ensure ongoing alignment with our internal policies, established standards, and compliance obligations. These reviews help verify that security controls remain effective, consistently applied, and appropriately maintained.

4.4 Continuous Improvement

We actively incorporate lessons learned from audits, technical assessments, industry trends, and threat intelligence. These insights help refine our processes and maintain a strong, adaptive security posture.

5 Incident Management

Kariera Group maintains a robust, structured, and well-governed Incident Management Framework designed to ensure that any security or privacy issue is identified, thoroughly assessed, and managed with the highest level of diligence and professionalism.

Our approach reflects our commitment to safeguarding customer trust, maintaining service continuity, and fulfilling all regulatory obligations, including those under the GDPR.

It ensures that incidents are handled efficiently, transparently, and in a manner that supports continuous improvement.

6 Compliance

6.1 ISO/IEC 27001:2022 Alignment

Our information security practices are aligned with the principles and requirements of ISO/IEC 27001:2022. This ensures a systematic, risk-based, and comprehensive approach to managing information security across all areas of the organization.

6.2 GDPR Compliance

Kariera Group fully adheres to the requirements of the General Data Protection Regulation (GDPR).

We uphold the principles of lawful and transparent processing, data minimization, and accountability, while ensuring that individuals can exercise their rights effectively.

Our processes and controls are designed to protect personal data throughout its lifecycle and maintain compliance with all applicable obligations.

6.3 Supplier Management

Suppliers and third-party providers play an essential role in supporting our services. We conduct structured evaluations and ongoing monitoring to ensure that each partner maintains a security and privacy posture that meets Kariera Group’s expectations and complies with relevant regulatory requirements.

7. Conclusion

Our commitment to information security and data protection is integral to our mission and business operations. We strive to maintain the trust of our clients and stakeholders by upholding high standards of security, privacy, and compliance.

Version 1.0, last updated November 2025