GARDIN

Information Security at Gardin

Whitepaper

Introduction

The security of Gardin customer and partner data is our top priority. To this end, the company has built itself, from an early stage, around a robust information security framework to ensure the integrity and safety of all data managed within our company and our products.

This whitepaper outlines the security measures we employ, reflecting our commitment to maintaining stringent security standards. Its intention is to provide transparency to Gardin's customers and partners regarding the security protocols we have put into place and how they are managed within our operations.

For any further questions or details, please contact the Gardin Security team at security@gardin.ag.

GARDIN

Table of Contents

1. Security at the core of the organisation

1.1 Information Management System

Gardin has established an Information Security Management System (ISMS) that aligns with the International Standards for Information Security (ISO/IEC 27001).

This ISMS serves as the strategic framework guiding the implementation of our information security processes and the technical measures we adopt. Additionally, the ISMS provides a comprehensive overview of all security measures in place and acts as a vital tool for the continuous enhancement of Gardin's security posture.

Gardin adheres to stringent policies and procedures, considering the confidentiality, integrity, and availability of our systems and services.

1.2 Compliance and Risk Management

Gardin has established a dedicated Security Working Group (SWG) team to ensure compliance with relevant standards, headed by an appointed virtual Chief Information Security Officer (vCISO) who has overall responsibility for the Information Security Management System (ISMS) and compliance workstreams. The vCISO reports directly to the CEO, ensuring that strategic security priorities align with our company's executive leadership.

Gardin maintains compliance with key standards related to information security and privacy, including:

- ISO/IEC 27001:2022
- GDPR
- Cyber Essentials Plus

We conduct continuous risk assessments across our environments and products to identify current threats and ensure that our controls are effectively managing these risks. The approach to these risk assessments varies depending on the specific environment or product under review - for instance, product assessments might typically involve technical risk assessments or code reviews.

Additionally, we extend our evaluations to include broader business risks, ensuring a comprehensive risk management strategy. As part of our risk management program, we carry out an annual risk assessment, conducted by our SWG team. Based on the outcomes, we initiate projects at least quarterly to mitigate any identified risks, thereby strengthening our overall security posture.

1.3 Security Operations Centre

Gardin has appointed a managed Security Operations Centre (SOC) that provides 24/7/365 monitoring and detection of threats across our corporate networks, electronic locking systems, and broader infrastructure. The team of trained security analysts continuously monitors internal and external threat intelligence data to detect anomalies and suspicious activities that could indicate a security breach or attempted intrusions. Detected threats are managed based on predefined rules that determine their severity and the urgency of the response required. Where necessary, threats are escalated into the internal Gardin Security Team for rapid remediation.

In the event of a severe threat discovery or an ongoing attack, Gardin has access to an emergency protocol that includes a 24/7 "panic button" feature, allowing for immediate escalation and rapid deployment security experts from the SOC team, ensuring that any critical situation is addressed promptly and effectively.

1.4 Employee Background Checks

At Gardin, we want to hire people who will actively contribute to and enhance the security-focused culture we've established. In alignment with local laws, we conduct background checks on all new hires to support this objective. Depending on the specific role, these background checks may encompass criminal history, educational qualifications, previous employment verifications, and, when relevant, credit checks.

1.5 Security Awareness Training

All staff members receive security awareness training as part of their onboarding process and are required to complete refresher training annually to keep security at the forefront of their daily activities. Our security awareness training program covers a range of topics, including current threats and scams, secure working practices, behaviours that pose security risks, and compliance with regulatory issues such as GDPR. Depending on their role, staff may undertake additional specialised information security training, centrally coordinated through the Security Working Group (SWG) and HR teams.

Furthermore, all employees receive ongoing security updates through informational emails, talks, presentations, and a variety of resources available on our intranet to maintain a high level of security awareness across the organisation.

1.6 Physical security

Gardin controls access to its offices and facilities using access cards, locks, and alarm systems. Each door access is attributable to a named member of staff and/or contractor, and strictly granted based on their 'need-to-know' and specific role requirements.

Visitors are accompanied throughout the facilities to ensure security. Our Human Resources (HR) department is responsible for assigning employees and contractors to their respective roles and access to Gardin's offices and facilities. This team in collaboration with the vCISO conducts periodic reviews of access card assignments to maintain security integrity and all access logs are closely monitored by our dedicated Security Operations Centre (SOC) team.

Additionally, alarm systems are strategically implemented to control and monitor access within Gardin facilities.

2. Securing our infrastructure

2.1 Cloud-first

A guiding principle at Gardin is to utilise cloud services wherever possible for the design, development, and hosting of our products.

We use Amazon Web Services (AWS) to provide our cloud infrastructure, benefiting from its high security standards as demonstrated by the over 140 compliance certifications listed on the AWS website. AWS provides us with secure data centres, robust physical infrastructure, and standardised infrastructure components, meaning our engineers can focus on developing secure and reliable products that address our customer’s unique challenges.

Gardin works closely with our dedicated AWS account manager and Business Support team to keep up to date with the latest best practice in secure cloud architecture design, and our Security and managed SOC teams are proactive in ensuring we are always prepared and responsive to the evolving security landscape by subscribing to AWS Security Bulletin updates.

The relationship between AWS and its customers pertaining to cloud security is defined through the Shared Responsibility Model. The AWS Shared Responsibility Model delineates the division of security responsibilities between AWS and its customers: AWS manages the security “of” the cloud, covering the

physical infrastructure, network, and hypervisor, while customers are generally responsible for security “in” the cloud, which includes their data, applications, configurations and where necessary, operating systems. For abstracted services, which Gardin utilises wherever possible, AWS also oversees the operating system and platform layers, leaving customers only responsible for securely accessing the hosted endpoints to store and retrieve data and the use thereof.

For internal and line-of-business applications, such as those used by our Finance and HR teams, Gardin employs reputable third-party SaaS platforms. These services are selected through a rigorous cloud vendor due diligence assessment process, ensuring they meet our high standards for security and functionality.

2.2 Network security and redundancy

Gardin employs a multi-layered security strategy across our networks, organising our infrastructure into distinct zones, environments, and services, each with specific security controls in place. These include zone restrictions that limit network traffic among office staff, customer data, CI/CD processes, and demilitarised zones (DMZ). We work closely with our Internet Service Provider (ISP) to ensure the same protections are applied to our WAN connections with the wider internet.

To further enhance security, we enforce environment separation, restricting connectivity between production and non-production environments. Access to production networks and services is tightly controlled, allowing only services within the same network to communicate with each other.

Inter-service communication is managed through virtual private cloud (VPC) routing, firewall rules and software-defined networking, ensuring that only explicitly authorised services can interact with one another. All connections to these networks are fully encrypted, which is globally enforced through service control policies (SCPs). Additionally, we have implemented intrusion detection systems in both our internal and production networks to swiftly identify and address potential security breaches. Regular network scans audit for open network ports and IP addresses and the results are reported directly to the Security team for assessment.

All critical components of Gardin’s environment and services are designed to be highly available, ensuring robust and reliable performance. For our cloud-based networks, we use availability zones within Amazon Web Services (AWS) to ensure network redundancy within the same region.

2.3 Management of compute services

One of our strategic information security objectives is to minimise as much a possible the use of internally configured servers, whether physical or virtual.

Instead, we prioritise the use of abstracted cloud-based compute services, including serverless and containerised architectures, as much as possible. This approach shifts the responsibility for managing and securing the underlying servers to our cloud provider, Amazon Web Services (AWS).

If the use of server instances is unavoidable, before deployment into production all servers are hardened to enhance security. This process includes disabling any unused services and network ports, as well as changing default passwords and enforcing SSH-key authentication. Additionally, to maintain consistency and security across our infrastructure, all instances adhere to uniform group policies and are subject to regular automated patch management provided through our cloud provider and associated security partner(s).

2.4 Identity and access control

Gardin applies the principles of ‘least privilege’ and ‘need to know’ in managing access to systems and information. Access rights are only granted following a formal request and must receive the requisite management approval. Additionally, these access rights are subject to periodic reviews controlled by the vCISO to ensure they remain appropriate and secure.

Access to Gardin’s production environment is regulated through Identity and Access Management (IAM) and is managed on a ‘just-in-time’ basis. This means that access is provided only when needed and only for the duration necessary, enhancing security and reducing exposure. Continuous monitoring of system access is conducted by our SOC team and suspicious activity is investigated and escalated accordingly. Furthermore, multi-factor authentication (MFA) is enforced for all Gardin employees and contractors across all applicable systems to minimise unauthorised access through stolen credentials.

3. Data security

3.1 Encryption

All customer data in transit across both the private Gardin network and public networks are encrypted in transit using Advanced Encryption Standard (AES) 256 encryption algorithms and Transport Layer Security (TLS 1.2) or better.

Gardin uses the AWS Key Management Service (KMS) for key management. The encryption, decryption, and key management process is inspected and verified internally by AWS on a regular basis as part of their existing internal validation processes.

When at rest, data is protected using industry-standard AES-256 full-disk encryption. This applies to all cloud/server data storage and local hard disks (i.e. those present on staff workstations).

3.2 Retention

Gardin does not retain data longer than necessary for the purposes for which it is processed. If a customer agreement is terminated, Gardin will promptly return or destroy all confidential information of the customer upon their request, in accordance with our general Terms and Conditions.

For personal data, Gardin adheres to the General Data Protection Regulation (GDPR) and ensures that data is not retained longer than necessary for the purposes for which it is processed, except when required to comply with legal obligations, such as statutory retention periods. For more detailed information on how we handle personal data, please refer to our Privacy Policy.

3.3 Tenant isolation

While our customers share a common cloud-based infrastructure when using Gardin's products, we have measures in place to ensure they are logically separated so that the actions of one customer cannot compromise the data or service of other customers.

Gardin employs a bridge tenant isolation model. In this model, while customers share certain components of the underlying infrastructure—such as a monolithic web application—they also benefit from dedicated resources, like individual application databases. In situations where tenant data is physically co-located, such as in a centralised data warehouse, it remains logically separated. This is achieved through row or object-level access control, which is reinforced by each customer's unique tenant ID.

Each customer is designated as a "tenant" within the Gardin data ecosystem and assigned this unique tenant ID. This ID ensures that all data specific to a tenant is distinguishable from that of others, without revealing any public identities. This mechanism allows Gardin to enforce stringent access controls over customer user accounts and Gardin employees alike, with 24/7 monitoring and intrusion detection in operation through our SOC team.

3.4 Audit logs

Gardin utilises comprehensive audit logging to track user activity across our systems, particularly in relation to accessing and manipulating customer data. To safeguard the integrity of these logs, they are stored in an isolated account

structure where access is tightly controlled. Access to these logs is always read-only to prevent any possibility of tampering. Furthermore, these audit logs are integrated into our Security Information and Event Management (SIEM) solution enabling continuous 24/7 monitoring, facilitated by automated rules and overseen by our Security Operations Centre (SOC) team.

4. Application and product security

4.1 Change management

All development activities across both software and hardware, including issue remediation and patching, are governed by our Change Management Policy. Defined by the Gardin Engineering team, this policy mandates that all system changes are thoroughly tested and authorised before being deployed to production environments. Authorisation of changes as “ready to deploy” must be given by the CTO before deployment can begin.

4.2 Secure development practices

Our software development lifecycle (SDLC) emphasises strict adherence to secure coding practices and includes both automated testing and manual peer reviews to screen software changes for potential security issues. Code changes are tracked using a version control system and must undergo quality assurance (QA) testing to confirm that all security requirements are satisfied. Only after successful completion of the QA process are new changes considered ready for release. Wherever possible, the SDLC prescribes the use of automated deployment strategies to maintain a consistent staging and release process, minimising deployment failures due to human error.

Upon release, changes are logged, archived, and notifications are automatically sent to the management of the Gardin Engineering team.

Additionally, access to Gardin’s production infrastructure is strictly limited to authorised personnel only. Security configurations and access rights are regularly reviewed by our Security team to maintain the integrity and security of our production environments.

4.3 External security testing

Gardin engages an independent specialist cyber-security organisation to undertake regular (at least annual) penetration testing of our internal and external

systems. These tests are conducted by security experts specialising in the technology stack(s) under test, and are guided by industry-recognized methodologies such as the Open Web Application Security Project (OWASP).

In addition, the Security and Engineering teams work in collaboration with third-party consultants to provide technical security assurance of high-priority projects - for example, a new product feature, new infrastructure setup or re-architecture.

5. Operational security

5.1 Vulnerability management

Our Security team conducts regular automated and manual security testing and patch management in conjunction with the Engineering teams. We also collaborate with third-party specialists to identify and address potential security vulnerabilities.

As an integral part of our information security management system, findings and recommendations from these assessments are communicated to Gardin senior management. Each finding is evaluated and prioritised based on their risk level, and are tracked until fully remediated, either through patching the vulnerable systems or implementing other relevant controls.

5.2 Supplier risk management

Where Gardin engages any third-party suppliers, including contractors and cloud service providers, our Supply Chain Operations teams conduct a thorough review process prior to awarding of contracts. For engagements deemed high or critical risk, additional reviews are carried out by our Security Working Group and where necessary, our managed Legal team, and must be approved by senior management.

We have a dedicated cloud vendor due diligence process that ensures prospective third-party services comply with our minimum security requirements before engaging with us. These requirements include encryption for data in transit and at rest using non-deprecated algorithms, and the implementation of sufficient audit trail mechanisms to provide Gardin with relevant information regarding potential security incidents.

Ongoing due diligence is conducted through subsequent reviews, either upon contract renewal or annually, depending on the risk level of the engagement.

5.3 Service availability

For our external and public services, Gardin is committed to maintaining transparency with our customers regarding service availability. We provide real-time updates on our dedicated status page, accessible at: https://status.gardin.ag.

In the event of incidents with medium or higher severity, we conduct a thorough analysis and subsequently publish a post-mortem. This report is made available after the issue has been successfully remediated. The level of detail included in each post-mortem is carefully calibrated to provide comprehensive insights to foster understanding and trust, whilst also guarding against disclosing information that could potentially be exploited by malicious actors. This balanced approach helps us to ensure ongoing transparency while protecting the security and integrity of our services and customer data.

5.4 Continuous logging and monitoring

Gardin employs a SIEM (Security Information and Event Management) platform to aggregate logs from various sources across our infrastructure (including audit, event and error logs) applying specific monitoring rules to these logs to identify and flag any suspicious activities. These flagged activities are then reviewed by our managed Security Operations Centre (SOC) team. Established protocols outline the procedures for triaging these alerts, conducting further investigations, and escalating them as necessary. Key system logs are forwarded in a read-only format from each system to maintain data integrity and prevent tampering.

The SOC team actively creates alerts on our security analytics platform and vigilantly monitors for any indicators of compromise. Both our Security and Platform teams utilise this platform to monitor not only for security threats but also for any availability or performance issues that may arise.

5.5 Securing our endpoints

Gardin utilises endpoint management software to centrally deploy updates and patches to operating systems and key applications across our endpoint fleet. Remote configuration of endpoint security policies is also achieved through the same approach. The Gardin IT team continuously monitor the compliance of all endpoints against the company's security rules, and any endpoints that fall out of compliance are immediately flagged for attention and remediation, reporting back to the Security team for enhanced auditing and subsequent check-up reviews.

Company workstations are centrally configured to protect data at rest with full disk encryption. Additionally, we enforce a complex password policy to ensure strong security practices. Based on these policies, strong passwords and multifactor authentication (MFA) are also technically enforced across our systems, further securing access to sensitive data and resources.

To protect against malware, Gardin employs enterprise anti-malware technology that is automatically applied to all active endpoints. Alongside the detection and quarantining of malicious software, this solution enables the Gardin IT team to remotely isolate any endpoint demonstrating suspicious behaviour from the rest of corporate network and lock down access to block further attack vectors.

5.6 Provisioning and disposal of hardware

Gardin procures its staff workstations and corporate network infrastructure through our IT managed service provider (MSP), which operates a secure vendor supply chain. Before being issued to staff, all workstations and other computers are configured by our IT team to ensure they have the appropriate security settings and approved applications installed. This process guarantees that each device meets our stringent security standards.

When hardware is taken out of service, it is securely decommissioned, with all hard disk drives being destroyed through a specialised hard drive disposal service to ensure that no data can be recovered. A certificate of disposal is issued for each item to ensure full traceability.

5.7 Disaster recovery and business continuity

Gardin recognises that disasters can occur at any time and in any location. To mitigate such risks, our infrastructure is designed for resilience, and we have contingency plans in place to address service-impacting events. We utilise Amazon Web Services (AWS), which operates across multiple data centres to ensure data and processing redundancy. Critical system and customer data is backed up daily, and our engineering team is notified of any backup failures, addressing issues promptly to maintain data integrity. Regular recovery tests

To meet information security requirements during a major crisis or disaster affecting Gardin operations, we maintain a comprehensive disaster recovery plan. This plan is reviewed annually by the Security Working Group (SWG), and selected elements are tested at least annually. Any relevant findings from these reviews and tests are documented and tracked until resolved.

Our disaster recovery strategy includes defining a Recovery Time Objective (RTO), which specifies the time frame within which business processes or services must be restored after a disaster, and a Recovery Point Objective (RPO), which sets the maximum tolerable period for data loss from a service

disruption. During Disaster Recovery testing, we also measure the Recovery Time Actual (RTA) to evaluate our performance against these objectives.

Additionally, we conduct annual Business Impact Assessments (BIAs) to evaluate the risks associated with our critical services. The insights gained from these BIAs inform our disaster recovery and business continuity strategies, enabling us to develop effective plans for critical services to ensure continuity and rapid recovery in the event of a disaster.

6. Management of security incidents

Gardin has a comprehensive approach to handling security incidents, which we define as any event that negatively impacts the confidentiality, integrity, or availability of customer or Gardin data and/or Gardin services.

As part of our incident response procedures, we have established a centralised chain of command and clear role assignments to ensure effective management of security incidents. Our process includes the following actions:

- Respond swiftly to alerts indicating potential incidents.
- Assess the severity of the incident.
- Implement mitigation and containment measures as required.
- Communicate with relevant internal and external stakeholders, including notifying affected customers relevant data protection organisations as required by relevant laws and regulations.
- Collect and preserve evidence for investigative purposes.
- Document a postmortem analysis and create a permanent triage plan.

In the event of a data breach containing personal data, Gardin notifies the relevant Data Protection Authority - the UK Information Commissioner’s Office (ICO) - within 72 hours of becoming aware than an incident has occurred, as is obligated under the GDPR and UK Data Protection Act 2018.

Our incident response processes are regularly audited as part of our ISO/IEC 27001 compliance assessments.