SECURITY PRACTICES

Security Classification: Public
Date: 25 October 2021
# TABLE OF CONTENTS

1. Introduction 3
2. Compliance 3
3. Our Information Security Objectives 3
4. Geekbot Security Practices 4
   4.1. Information Security Policies 4
   4.2. Roles and Responsibilities 5
   4.3. Human Resource Security 5
   4.4. Asset Management 6
   4.5. Access Management 6
   4.6. Encryption 7
   4.7. Physical Security 7
   4.8. Operations Security 8
   4.9. Network Security 10
   4.10. Design, Development and Support 10
   4.11. Data Retention 11
   4.12. Suppliers’ Relationships 11
   4.13. Incident Management 12
5. Conclusion 12
1. Introduction

Geekbot’s main goal is to make your days more manageable, by providing you everything you need in order to run effective standups, surveys, and reports. Since our mission is based on information exchanging, we are committed to ensure the safety and security of information provided and processed. Moreover, our team is dedicated to help our customers take full advantage of our services, ensuring at the same time their organization’s security.

This paper outlines how the Geekbot security team keeps our systems secure by staying focused on the concept of defense in depth, and by demonstrating compliance to international standards, regulations and best practices.

2. Compliance

Geekbot meets some of the most broadly recognized security standards, and focuses on security governance, risk management and compliance.

We are ISO/IEC 27001 certified, and we comply with the applicable Data Protection regulations (i.e., GDPR, UK-GDPR, CCPA). Our approach to security dictates that we will continue our efforts to ensure that we remain in compliance with the above-mentioned standards and regulations, as well as to constantly evolve with updated guidance and new industry best practices.

We continuously monitor, audit and improve the design and effectiveness of the security controls in place by engaging accredited third-party assessors, and by ensuring that all findings are tracked until their resolution.

Our goal is to maintain at all times the confidentiality, integrity and availability of the data, services and systems in place.

3. Our Information Security Objectives

Our information security objectives cover the controls we implement across a number of security domains, and the processes in place to ensure that our services meet and exceed our customers’ requirements.

Specifically:

• Our aim is to ensure the continuity of the provided services.
• We are focused on demonstrating compliance with international standards, regulations and best practices.
• Our purpose is to meet our customers' requirements in regards to the security of their information by maintaining clients' and stakeholders' confidence.
• Our team is dedicated to identifying and resolving any security incidents and service weaknesses, which are managed in accordance with relevant procedures.
• The raising of security awareness, training and motivation of the company's personnel are the main aspects of our security approach.


Geekbot's security team enforces globally recognized best practices and frameworks to keep your data and information secure. This includes an information security policies' set, dedicated roles and responsibilities, human resource security practices, asset management and access control tools, encryption mechanisms both for data at rest and in transit, physical security controls, operations security controls, network security controls, security in development and support processes, as well as countermeasures to ensure information security in suppliers' relationships, incident management and business continuity. The management and handling of these issues are depicted in the next sections.

In order to ensure the effective implementation of the above, we continually evaluate our current approach to security, and we stay focused on identifying opportunities for improvement by undertaking a number of maturity assessments using independent security consulting companies. We also have in place metrics and KPIs (Key Performance Indicators) to timely identify gaps and target any areas for improvement.

4.1. Information Security Policies

Geekbot information security policies apply to all the company's systems, people and processes, including board members, directors, employees, contractors and other third parties who have access to Geekbot information systems.
Geekbot is committed to the effective implementation and provision of resources for the improvement of all information security aspects within the organization.

The information security policies in place aim to ensure:
• The continuous protection of information against unauthorized access.
• The confidentiality and integrity of Geekbot's information, clients and partners.
• The availability of information and business transactions.
• The monitoring and compliance with the legislative and regulatory requirements concerning Geekbot.
• The adequate training of the Geekbot employees in information security issues.
• Compliance is mandatory for all parties that have been or are cooperating with Geekbot.
• Technical and organizational measures are in place, and implemented.

All Geekbot information security policies are reviewed at regular time intervals (at least once a year) to ensure their adequacy and that they are fully followed.

4.2. Roles and Responsibilities

Within our information security management system there are a number of roles, each with their own responsibilities, which are allocated to specific individuals or groups within the company. Geekbot’s security team is led by our Chief Information Security Officer (CISO) who is responsible for the implementation and management of the company’s security program. The rest of the members of the Geekbot’s security team, who support the CISO, are responsible to ensure that focus is given on Security Architecture, Security Engineering and Development, day-to-day Operations, and Risk and Compliance.

A dedicated member of our security team is the Data Protection Officer (DPO), who is responsible for the training of employees on issues regarding data processing, and for conducting regular audits to ensure the company’s compliance with data protection requirements. The DPO also serves as the point of contact between the company and the relevant supervisory authorities.

4.3. Human Resource Security

Geekbot aims to ensure that all employees and contractors who operate on behalf of the company understand their responsibilities and they are suitable for the roles for which they are considered. All staff involved in information security are competent on the basis of appropriate education, training, skills and experience.

The skills required are determined and reviewed on a regular basis together with an assessment of existing skill levels within Geekbot.

Background verification checks on all candidates for employment are carried out in accordance with relevant laws, regulations and ethics. Depending on the role, background checks may include criminal history checks, education verifications, and employment verifications.

Additionally, Geekbot’s contractual agreements specifically state both the employees’ and the company’s information security responsibilities prior to, during and upon termination of employment.
Geekbot provides to all employees and contractors the support they need to continuously build and increase their knowledge regarding security issues and threats they need to be aware of. Training needs are identified, and a plan is maintained to ensure that the necessary competencies are in place.

To this end, all Geekbot staff is required to participate in security awareness training on an ongoing basis, including topics relevant to uprising threats, secure working practices, potentially risky behaviours, as well as compliance issues. On top of that, Geekbot conducts more targeted training courses aiming to increase our developers’ awareness regarding secure coding practices.

Formally training and awareness programs are performed via the use of the internal survey mechanism.

**4.4. Asset Management**

Operational procedures are used for the maintenance of Geekbot's information systems and infrastructure in order to ensure the maximum possible utilization of its assets.

For systems which are located in infrastructure obtained through cloud service providers, the appropriate SLAs (Service Level Agreements) are in place to ensure the adequate protection of the information processed, transmitted, and stored. Software and application development and testing environments are separate from the active production environments, to reduce the risk of accidental changes as well as unauthorized access to data.

**4.5. Access Management**

Geekbot’s access management controls are enforced taking into consideration the principles of least privilege and role-based permissions when provisioning access. All employees are only authorized to access data that they are required to handle in order to manage the responsibilities that fall under their job descriptions. When an employee leaves Geekbot, their access to information systems is suspended upon completion of the last day of their work.

Each user has a unique username and password, and the use of shared accounts is generally forbidden. Access to information systems is through this unique username that can be associated with a particular individual, and access to servers is controlled by a secure connection process. User access to information systems is monitored and recorded, while users’ access rights are reviewed at regular time intervals.
Geekbot uses multi-factor authentication for all access to critical systems, and private keys for authentication (where applicable). An approved password manager is used in order to generate, store, and enter unique and complex passwords, and Geekbot password policy is enforced to all information systems enabling password complexity and regular password changes. Additional procedures to ensure the correct use of administrators' accounts are in place.

Remote access of suppliers/partners to Geekbot's information systems is also controlled through the company's access control procedures. Any remote access software is disabled when not in use.

**4.6. Encryption**

Geekbot encrypts both data at rest and data in transit by using strong encryption algorithms based on best practises, such as AES-256, RSA-2048, and Strict Transport Security (HSTS). Additionally, SHA-256 is used for all applications that employ secure hash algorithms.

All servers and applications use SSL or TLS having certificates signed by a known, trusted provider. All cryptographic keys are generated and stored in a secure manner that prevents modification, loss, destruction, theft, and unauthorized disclosure or compromise. Cryptographic keys that are used in test and developing environments are not used at the production environment.

**4.7. Physical Security**

Our Risk Assessment determines the appropriate level of protection that needs to be in place to adequately safeguard the data stored in Geekbot premises. The company’s Physical and Environmental Security Policy sets out the protection measures that need to be taken to create a safe space and explains how one should take care of it, so that this space remains safe.

Any documents kept at offices accessible to all staff and / or external visitors are protected by physical access control measures, including locked cabinets and protected safe areas.

Computer equipment resides in appropriate physical locations to limit environmental risks, to reduce the risk of theft, and to limit the risk of unauthorized people accessing information and data. Equipment of the information systems is maintained in accordance with the manufacturer's instructions and in accordance with documented internal
procedures to ensure that it remains in good condition.

For Geekbot services which reside in the cloud, the data centers are maintained by industry-leading service providers who offer an adequate physical protection of servers and infrastructure and Security Certifications are in place (i.e., ISO 27001, SOC 2 reports, etc.).

4.8. Operations Security

4.8.1. Change Management
All major changes to the basic infrastructure (e.g., network, servers) are considered for the impact they may have on the security of Geekbot information, and they are managed in accordance with our change management procedure.

All upcoming changes and/or major upgrades to Geekbot information systems are first tested in a dedicated test environment which is a precise simulation of the production environment prior to their implementation in the Geekbot production environment. Once the changes prove correct and complete, then they are transferred to the production environment.

4.8.2. Capacity Management
Information systems and facilities are covered by a needs forecasting plan, and by equipment replacement procedures that ensure that increased power and data storage requirements can be addressed and met in acceptable time.

4.8.3. Protection Against Malicious Code
To reduce the risk of virus infection the following protection measures are applied:

- Evaluation of virus protection software prior to purchase.
- Installation of antivirus software on all devices, e.g., servers and workstations, including laptop computers, tablets and smartphones.
- Implementation of emergency procedures for dealing with virus incidents, so that the virus spread is stopped and adequate measures are applied.
- Configuration of security settings which reduce the risk of malicious code infections (e.g., disable autorun or browser configuration).

All Geekbot employees are aware of the ways in which malware enters and infects devices, the risks that malware poses, the inability of technical controls to prevent all incidents and the importance of users in preventing incidents.

4.8.4. Backups
Regular backups of key business information are taken to ensure that Geekbot can recover from a disaster, digital media failure or the consequences of a human error.
A suitable backup cycle, which is well documented, is in place.

4.8.5. Logging and Monitoring
Geekbot monitors servers, workstations and mobile devices to log administrative access, use of privileged commands, and system calls on all servers in Geekbot’s production network.

Log entries contain at least the following information for each event, where available:
- User ID;
- Event date and time;
- System identity (e.g., name and/or IP address);
- Event-related information (message or code);
- Event success or failure indication.

Logs that record security-related exclusions and events are kept for at least six (6) months as required by the relevant legislation.

Access to logs is protected against unauthorized access, and system administrators are not allowed to delete or disable logs of their own activities.

Logs also include backup times, along with details of how to change your backup media, the boot and shutdown events of any system and any user involved, and system errors (type, date, time), along with corrective actions.

4.8.6. Endpoint Security
All workstations issued to Geekbot personnel are properly configured in order to comply with the company’s security requirements. All workstations are regularly updated, all hard disks are encrypted, strong passwords are enforced, and workstations are locked within a specific time of inactivity.

Antivirus mechanisms are enabled to all workstations, and configurations are in place to ensure that potential malware and/or unauthorized software are reported. Geekbot does not accept the use of non-licensed software.

4.8.7. Security Assessments
Security assessments on Geekbot’s information systems are carried out at least once a year, including the following:
- Authenticated and unauthenticated Penetration tests.
- Infrastructure scans.
- Analysis of vulnerabilities, patches, vulnerable access codes, and network services.
• Analysis of exploitation of vulnerabilities.

Vulnerability Assessments and Penetration Tests are performed by independent entities in order to ensure that potential security weaknesses are identified and properly mitigated. This is performed for all critical applications and before their installation at the production environment.

4.9. Network Security

Network security management is vital for providing services. Connections to Geekbot's network infrastructure are made in a controlled manner. Networks are segregated based on Geekbot business levels, and firewalls and Virtual LANs (VLANs) are used where appropriate. All critical infrastructure components are fenced by security controls (i.e., Firewall, etc.).

4.10. Design, Development and Support

Coding standards are documented for all coding technologies used in Geekbot development projects. These coding standards are followed by all developers writing or reviewing code. Training is required to ensure that all relevant personnel are sufficiently aware of the coding standards.

All data entered into Geekbot information systems, either manually or automatically, are validated, when appropriate, with input checks such as boundary checking or limiting input fields to specific ranges or values. Applications incorporate validation checks in business rules, to avoid errors or inconsistencies in multiple routines. Data validation is performed at the server level to protect against malicious data coming from compromised clients, and it is based on best practices, such as OWASP Application Security Verification Standard Project and OWASP Testing Guide. Integrity checks are also in place to permit validation of output data.

Software development and testing environments are separated using appropriate controls, including:
• Running software on different infrastructure components and different networks.
• Use different accounts and test data.

New products are procured through predefined procedures. New information systems, product upgrades, and software fixes undergo proper control prior to their acceptance and availability in the production environment. Third-party applications are tested for possible service packs, as well as for individual patches.
Major upgrades of information systems are thoroughly tested in a safe test environment, as a copy of the production system.

4.11. Data Retention

All records held by Geekbot are categorized and depicted in the company’s retention policy and respective records. There may be specific circumstances where records need to be kept for a longer or shorter period. This is decided on a case-by-case basis as part of the design of the information security elements of new or significantly changed processes and services.

Geekbot implements a cryptographic control policy which is reviewed annually, in order to protect the confidentiality and integrity of all records which are maintained. Depending on the classification of information and the storage location, appropriate cryptographic techniques are implemented.

Once records are no longer necessary, they are securely destroyed. Specifically, destruction of all records, regardless of the media, is conducted in a secure manner to ensure there are safeguards against accidental loss or disclosure. The approval of the destruction is recorded, in addition with all the necessary details and retained as evidence.

4.12. Suppliers’ Relationships

In cases where the presence of sub-service organizations is required, then Geekbot takes all the appropriate countermeasures to ensure that the company’s information security posture is maintained by establishing agreements that require from our suppliers/vendors to adhere to confidentiality commitments.

Specifically, written contracts exist between all parties involved, and each supplier contract describes as accurately as possible the exact services provided to Geekbot. Appropriate Data Processing Agreements (DPA) or standard contractual clauses are in place with all of our sub-processors. The information security requirements and security controls are formally documented in the contractual agreement which may be part of, or an addendum to, the main commercial contract.

Non-Disclosure Agreements are used in order to ensure the protection of confidential Geekbot information, and the basic principles of information security, such as less privileges and segregation of duties, are applied throughout the duration of the project. Additionally, Geekbot has the right to audit the information security practices of the supplier and, where applicable, its subcontractors.
4.13. Incident Management

An information security incident is any event that may result in loss of corporate information assets by any means. In the event of a security incident, the Geekbot responsible security team must be promptly informed by anyone who notices the incident. All security incidents are managed by our dedicated Incident Management Team (IMT) whose members are responsible to perform an investigation in order to identify the source of the incident, and collect evidence that can be used legally for future actions against the source. The evidence may also serve as evidence for disciplinary actions against employees. Depending on the criticality of the incident, the IMT will decide on the corrective measures, and on the preventive actions to be applied to avoid reoccurrence.

In the event of a data breach, a dedicated procedure is in place to ensure that all affected parties will be timely notified in accordance with the applicable legislation.


Geekbot implements the appropriate procedures in order to manage in a controlled and structured manner a serious crisis that could cause a cessation of operations, and to ensure that the company can effectively recover by an unwanted catastrophic event that could have a serious impact on the confidentiality, integrity or availability of its business processes.

The Geekbot Management approves the development and documentation of analytical procedures and the creation of the necessary infrastructure to ensure the continuity of business operations through an organized and integrated Business Continuity Management Framework in the event of a downtime of Geekbot Information Systems and business processes. Additionally, Geekbot Management provides the necessary resources for the development, implementation and maintenance of the BCP.

5. Conclusion

Geekbot has in place and implements all necessary technical & organizational controls to ensure the protection of your data. Keeping our customers’ information secure is of the utmost importance for us, and we are making our best effort to maintain and increase our accountability.

Please contact us at security@geekbot.com for any questions or concerns.