gravyty

your force for good

Information Security Policy

Version 1.4

Version 1.4. | 2023

Table of Contents

1. Purpose

1.1. The purpose of this policy is to outline the governing security and confidentiality policy, including the principles and rules related to the protection of information assets, to be followed by Headhunter Systems Limited ("**Gravyty**") personnel and other persons associated with the company.

1.2. Effective implementation of this policy will protect Gravyty and Gravyty's clients' proprietary and confidential information and technology.

2. Scope

2.1. This policy applies to personnel (employees, contractors, business partners, consultants, temporaries and others) who acquire, develop, install, maintain or use the company's systems and/or applications and to organizations connected to any owned network domain.

3. Intellectual Property Reference

3.1. All product names, trademarks and registered trademarks are the property of their respective owners. All company, product and service names used in this policy are used for identification purposes only. Apple, Mac, MacBook and iMac are trademarks of Apple Inc., registered in the U.S. and other countries. Microsoft, Windows, Office, Excel, Word and Outlook are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

3.2. All other trademarks cited herein are the property of their respective owners.

4. Roles & Responsibilities

4.1. Gravyty's management is responsible for:

- Defining and approving the company's information security vision, objective, maturity, policy, roadmap, strategy and work plan.

- Allocating resources to implement the Information Security work plan.
- Measuring information security progress to maturity on a periodic basis.
- Supporting Gravyty's information security policy enforcement.
- Gravyty's managers are responsible for:
- Ensuring that their employees adhere to the company's information security policy, guidelines and procedures.
- Ensuring that all employees are familiar with and working according to Gravyty's information security policies and procedures.
- Making information security considerations when managing their responsibilities.

4.2. Gravyty's employees are responsible for:

- Reporting any security threat, breach, incident or disclosure ASAP.
- Behaving according to the published information security procedures.
- Taking all necessary actions to ensure the security and confidentiality of both customers' and Gravyty's information to which they are exposed while working in the company.

Any employee found to have violated this policy may be subject to disciplinary actions.

4.3. Contractors and third parties are responsible for:

- Maintaining a high level of information security, contracts and SLAs.
- Behaving in accordance with all contracts and SLAs.

4.4. The Information Security Manager is responsible for:

- Planning, implementing and auditing, within the preventive detective and recovery cycles that match the executive management's mission statement and risk-taking policy.
- Ensuring that this policy is reviewed, updated and communicated to all employees.

5. Risk Management

5.1. General

5.1.1. Risk management is a continuous process that allows for the protection of Gravyty's information, systems and products. It enables the implementation of the necessary controls to protect organizational information assets, minimizing organizational exposure to related threats and associated risks.

5.1.2. This risk management process is to be performed on a sample and periodic basis to provide Gravyty's management with a view of the main information security risks related to sites and activities.

5.1.3. The risk management process is to cover Gravyty's business domains (Corporate, Customers and Development), business processes and IT assets (Systems, Servers, etc.).

5.1.4. The risk management process is also to cover Gravyty's products. Minimizing such risks is about to prevent attacks that can pass through network defenses directly to the application. Gravyty's products' security risk management is essential for sensitive customer data protection when products are used by Gravyty's customers and related services are provided by Gravyty's employees.

5.2. Risk assessment

5.2.1. A periodic audit should be conducted to maintain a high level of information security and to identify weaknesses and vulnerabilities that may expose data and equipment to external and internal threats that may lead to the interruption of business processes. Such an audit should determine the likelihood and impact of all identified risks using qualitative and quantitative methods.

5.2.2. The information security auditing cycle is to be conducted as follows:

- Annual assessment – comprehensive information security audit including penetration tests, vulnerability scans and reviewing compliance and effectiveness of information security practices and controls.
- Ad hoc assessment – specific auditing based on identified needs.

- Based on the above, an annual information security work plan is to be conducted. The work plan's priorities are to be based to a large extent on assessment results, with crucial risks mitigated immediately upon their identification.

5.3. Risk mitigation

5.3.1. A remediation process is to be conducted after vulnerabilities are analyzed and risks are evaluated. For the purpose of remediation, a remediation plan is to be issued and a follow up process maintained.

5.3.2. Changes to the provision of services within the remediation process, including the maintaining and improving of existing information security policies, procedures and controls, shall be managed, taking into account the criticality of the business systems and processes involved and the re-assessment of risks.

5.3.3. Risk mitigation will include updates to security policies, procedures, standards and controls, as required, to ensure they remain relevant and effective.

6. Information Handling & Protection

6.1. Segregation of duties

6.1.1. The company is to ensure applicable separation of the management or execution of certain duties or areas of responsibility to decrease the potential for fraud, misuse, or incompetence in the production environment.

6.2. Controls against malicious code

6.2.1 All equipment and Systems must have standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected equipment must be immediately removed from the systems until they are verified as virus-free by the IT Management Group.

6.3. Endpoints and servers

6.3.1. All endpoints must have an anti-virus application installed. All servers must have an anti-virus application installed that offers real-time scanning protection of files and applications running on the target system if they meet one or more of the following conditions:

- Non-administrative users have remote access capability
- The system is a file server
- Share access is open to this server from systems used by non- administrative users
- HTTP/FTP access is open from the Internet
- Other "risky" protocols/applications are available to this system from the Internet at the discretion of the IT Management Group

6.4. **Mail servers**

6.4.1. Mail servers must have either an external or an internal anti-virus scanning application that scans all mail to and from the mail server. Local anti-virus scanning applications may be disabled during backups if an external anti-virus application still scans inbound e-mails while the backup is performed.

7. Anti-Spyware

7.1. All servers must have an anti-spyware application installed that offers real- time protection of the target system if they meet one or more of the following conditions:

- Non-technical or non-administrative users have remote access to the system and any outbound access is permitted to the Internet
- Non-technical or non-administrative users have the ability to install software on their own

8. Exceptions

8.1. Exceptions to above requirements may be deemed acceptable with proper documentation if one of the following conditions applies to the system:

- The system is a SQL server
- The system is used as a dedicated mail server
- The system is not a Microsoft Windows ® based platform

9. Protection of log information

9.1. All activities on company routers are to be logged.

9.2. Backup logs are to be created and are to be reviewed to verify that the backup was successfully completed.

9.3. Logging facilities and log information shall be protected against tampering and unauthorized access.

9.4. Access to log and monitoring of information security management systems should be restricted to authorized personnel.

10. Access control

10.1. Access control policy

10.1.1. Gravyty's access control policy is established, documented, and reviewed based on business and security requirements for access.

10.1.2. The policy establishes the following:

- Security requirements of accessing individual business applications.
- Information dissemination and authorization based on the "need to know" principle to satisfy security requirements.
- Relevant legislation and any contractual obligations regarding protection of access to data or services.
- Standard user access profiles for common job roles in the organization.
- Management of access rights in a networked environment that recognizes all types of available connections.
- Segregation of access control roles, e.g., access request, access authorization, access administration.
- Requirements for formal authorization of access requests.
- Removal of access rights following a role change or termination.
- Requirements for periodic review of access controls.

10.2. Production and data access

10.2.1. Access to production resources and data is to be permitted for a few select Gravyty employees authorized by the IT Management Group, and they are to manage the production environment and/or disaster recovery (backups). To gain access to the production environment, employees will authenticate using a Multi- Factor Authentication mechanism.

10.2.2. Gravyty Support and Customer Success personnel may also access the system through a dedicated web interface (rather than direct machine access) solely for the purpose of providing support to customers.

10.3. Remote Access Control

10.3.1. Remote access is to be granted according to the "need to know" principle and subject to the information security manager's approval.

10.4. Access rights control

10.4.1. An annual periodic review of the allocation of access rights initiated by each asset owner should be established and documented.

11. Password policy

11.1. Each user account is to be password protected.

11.2. Employees are to ensure that their access passwords remain protected.

11.3. Passwords related to cloud services are to be constructed in accordance with the cloud service password policy.

11.4. Passwords must be difficult for unauthorized entities to guess.

11.5. Employees must ensure that their access passwords remain protected.

11.6. Employee passwords must adhere to guidelines as published in our Password Security Policy.

12. Responsibility for company information assets

12.1. All company assets are to be accounted for and to have a designated owner.

12.2. Owners are to be identified for all assets and the responsibility for the maintenance of appropriate controls is to be assigned to them. The owner is to be responsible for the proper protection of the information asset.

12.3. Rules for acceptable use of information assets are to be established and implemented.

13. Data in transit

13.1. All sensitive data must be securely protected if it is to be transported physically or electronically.

13.2. Sensitive data must never be sent over the Internet via e-mail, instant chat or any other end-user technology.

13.3. If there is a business justification to send sensitive data via e-mail, via the Internet or via any other method, this should be done with authorization and by using a strong encryption mechanism (i.e. AES encryption, PGP encryption, SSL, TLS, etc.).

13.4. Data in transit is always to use HTTPS – the secure version of HTTP – meaning that all the traffic between the users and Gravyty's platform is to be encrypted. Non-encrypted access to the platform is forbidden.

14. Encryption

14.1. Gravyty supports the implementation of data encryption to protect confidential information.

14.2. Encryption is to be implemented using well-known industry standards.

14.3. Detailed encryption guidelines are included in the Encryption Policy.

15. Physical security

15.1. General

15.1.1. Gravyty's physical servers are managed by Amazon Web Services ("AWS"). AWS is widely regarded as employing industry standard protective measures to ensure the security of the physical servers they manage, and they are relied upon by thousands of technology providers around the world. More information regarding AWS's physical security measures can be found in the Physical access chapter in the following link:

https://aws.amazon.com/compliance/data-center/control s/

15.1.2. Gravyty's customer data is managed by Google Cloud Platform ("GCP"), which is widely regarded as employing industry standard protective measures to ensure the security of the physical servers they manage, and they are relied upon by thousands of technology providers around the world.

15.1.3. Access to the company's facilities must be safeguarded and monitored.

15.2. **Visitor and contractor access**

15.2.1. Visitors who require Internet or systems access will need permission from the IT Management Group. After credentials are arranged, activities on the network will be subject to this Information Security Policy. Visitor use of employee credentials is not permitted under any circumstances.

15.2.2. Remote Access to Gravyty networks are governed by this Gravyty Information Security Policy.

16. Laptop and portable media security

16.1. Laptops are not to be given to unauthorized individuals.

16.2. Any classified/sensitive information to be saved on a laptop must be stored on an encrypted disk.

16.3. To prevent theft, laptops are not to be left unsupervised.

16.4. When not in use, laptops are to be locked and secured.

16.5. While using a laptop during a flight or in a public place, the user is to ensure that other people cannot view sensitive information.

16.6. When flying, employees are to always keep their laptops with them; laptops should not be stored in suitcases.

16.7. Employees are to take special care when undergoing security checks at the airport, particularly when they are required to put items through X-ray machines.

16.8. When staying at hotels, the laptop is to be kept in a hotel safety deposit box. If such a facility is not available, the laptop is to be locked in luggage.

16.9. Laptops are never to be left in a car, even if the car is locked.

16.10. Employees are advised to take their laptops home at the end of the workday. When left at the office, the laptop must be shut down and locked in a closet.

17. Software installation

17.1. Employees are not to install software on equipment that operates within the network or has access to its systems. Any non-standard software requests must first be approved by the requester's manager and then be made to the IT Management Group in writing. The IT Management Group will obtain and track the licenses, test new software for conflict and compatibility and perform the installation.

17.2. This section covers all equipment including computers, servers and other computing devices that operate within Gravyty's network or that otherwise have access to its systems.

18.E-mail security

18.1. E-mail usage is intended for work purposes only.

18.2. Every letter sent by e-mail must include a mail signature comprising the sender's name and telephone number.

18.3. Sending crude or insulting e-mail messages is prohibited.

18.4. Sending non-work-related data to anyone not interested in receiving such material is prohibited.

18.5. Using the company's internal distribution lists for private use is prohibited.

18.6. Sending sensitive documents by e-mail requires the use of the standard encryption approved by the company.

18.7. Automatic e-mail forwarding from the company to an external site is prohibited.

18.8. Using a reasonable amount of Gravyty's resources for personal e-mails is acceptable.

19. Client-side data and third-party hosting

19.1. Hosting of the client-side environment must be separate from the server side environment.

19.2. Client-side data must be stored in a separate database for each Gravyty customer.

19.3. Third-party hosting may be undertaken on behalf of Gravyty by one of the world's leading hosting providers. At the time of the writing of this policy, these are limited to:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

19.4. The third-party hosting providers must comply with all leading industry standards for information security, data protection and privacy, including but not limited to:

- ISO 27001, 27017, 27018
- SOC I, II, III
- GDPR
- Datacenter Physical Access Security
- Business Continuity / Disaster Recovery

20.HR Security

20.1. Pre-employment

20.1.1. Candidates for employment, contractor positions and third-party service provider users are to be adequately screened, especially for sensitive positions. Company employees, contractors, consultants and third-party service providers to information processing facilities are to sign an agreement regarding their security roles and responsibilities.

20.2. Employee termination

20.2.1. Employees' credentials are to be deactivated by the IT Management Group immediately upon termination of employment. This includes but is not limited to the following:

- Gravyty's database
- Workstation access

- E-mail access
- Remote access to Gravyty's network
- VPN client access
- Office access
- Any other kind of access to Gravyty's network or programs

20.3. Return of assets

20.3.1. The IT Management Group must collect all Gravyty equipment from employees before they exit the premises on their final day of employment.

20.3.2. The IT Management Group must update the equipment and systems inventory immediately to reflect the effect of the employee's termination.

20.4. Employee Security Awareness

20.4.1. The first line of defense in data security is the individual employee. Employees are responsible for the security of all data and access to systems to which they are exposed. The employee is responsible for participating in ongoing training and awareness programs held at Gravyty or elsewhere, from time to time. It is the information security manager's responsibility to inform all employees of these requirements, to notify employees of training and awareness sessions and to ensure adequate material and content is provided for employees to promote this activity. All employees are to confirm in writing, by signing off, that they have read the company's Information Security Policy.

21. Backup and Data Retention

21.1. Backup software is to be scheduled to run nightly to capture all data from the previous day.

21.2. Backup logs are to be reviewed to verify that the backup was successfully completed.

21.3. The IT Management Group shall designate a responsible individual to be available to ensure, daily, that the backups are running correctly. If the responsible individual is not available, an alternative individual should be designated to oversee the process.

21.4. Backup data storage are to be run and held off-site of Gravyty's physical premises. In the case of a disaster, backup tapes are to be available for retrieval and not subject to destruction.

21.5. Systems data is to be backed up daily.

21.6. The restoration process is to be tested regularly and written instructions should be created in the event the IT Management Group personnel are not available to restore data when needed.

22. Supplier Relationship

22.1. Information security in supplier relationships

22.1.1. Cooperation with suppliers can be an information security risk to Gravyty and must therefore be rigorously managed.

22.1.2. Prior to signing an agreement with an external supplier, the issue of whether the supplier requires access to Gravyty information or will be exposed in any way to Gravyty information or assets must be checked.

22.1.3. Any supplier who has access to Gravyty's resources is to sign an NDA.

22.1.4. In a case in which a contract with a vendor exposes that vendor to Gravyty's data, a security appendix is to be added to the contract, detailing requirements to provide information about the vendor's use of the information its method of protection. The appendix is to be written by the information security manager.

22.2. Supplier service delivery management

22.2.1. When applicable, all suppliers' access to Gravyty's resources are to be monitored.

22.2.2. Vendors and suppliers are only to have access to the systems, services, and information required to accomplish their tasks.

22.2.3. Upon completion of the contract with the supplier, the supplier's privileges are to be deleted from the relevant systems and the supplier is to return any identification devices that were used for strong identification, if any such devices were used, to Gravyty.

23. Network/Server Security

23.1. Network security management

23.1.1. The information security manager is to define the components required for Gravyty's network information security, to both protect the corporate network and the information stored in it, and to allow routine work to continue without interruption.

23.1.2. Each network element is to be hardened according to the industry's best practices.

23.1.3. The information security manager is to oversee network security and its various components.

23.1.4. Gravyty's IT manager is to centrally manage the computer network.

23.2. Separation of environments

23.2.1. Any data derivation from the production environment to other environments is to be authorized by the VP R&D and IT manager, whilst ensuring the environment is properly secured.

23.3. Security of network services

23.3.1. Security mechanisms, service levels and management requirements of all network services are to be identified and included in network services agreements, whether these services are provided in-house or outsourced.

23.4. Network access

23.4.1. Users and services connecting to the internal network from external, untrusted networks must be authenticated and be securely connected (via VPN or another application authentication mechanism). They are only to gain access to the services that they are authorized to use.

23.4.2. All connection points from Gravyty's network to external networks, and vice versa, must be approved by the VP R&D or the information security manager. All connections to trusted or untrusted external networks must pass through an approved firewall.

23.4.3. To eliminate a major vulnerability, all connections and accounts related to external network connections are to be periodically reviewed and are to be deleted as soon as they are no longer required.

23.4.4. Firewalls and/or security groups must be implemented for each Internet connection in the internal company network.

23.4.5. All inbound network traffic is to be blocked by default unless explicitly permitted. These restrictions must be documented.

23.4.6. No direct connection from the Internet to sensitive data is permitted. All traffic must pass through a firewall and make use of an authentication mechanism.

23.5. Network encryption

23.5.1. In any case, when applicable, encrypted protocols (i.e. SSH instead of telnet, https instead of http) must also be used when the transmitted data contains sensitive information.

23.5.2. All information must be encrypted during its transmission over wireless networks.

23.5.3. Exceptions must be authorized by the information security manager and the VP R&D.

24. Incident Management

24.1. Security-related events

24.1.1. Security-related events will be reported to the IT Management Group. Corrective measures will be prescribed as needed.

24.1.2. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences

24.2. Security incident handling

24.2.1. Once an event turns to be an incident, it is to be handled by the information security manager, who is to act to minimize the incident’s impact and to mitigate all related risks, keeping Gravyty's management updated in the process.

24.2.2. Every information security incident is to conclude with an exhaustive report which is to specify the following:

- Incident detection
- Response to the incident
- Neutralizing the endangering factors
- Drawing conclusions
- Documentation
- Lesson Learned

25. Business Continuity

25.1. Information security continuity

25.1.1. The Business Continuity Planning (BCP) process is designed to allow the continued proper operation of the business even when a catastrophe has occurred.

25.1.2. The BCP process is to include steps for continued protection of information and enable the continuation of operations even when the standard systems cannot continue routine work.

25.1.3. A Business Continuity test is to be carried out once a year in conjunction with Gravyty's management, with an emphasis on resources for which testing is essential.

25.1.4. The practice test is to be documented and investigated, and conclusions are to be drawn to improve the BCP process.

26. Redundancies

26.1. All company information is to be backed up regularly.

26.2. Gravyty's management is to define the availability required from every available computerized system and for each business process.

26.3. The Business Continuity Plan is to be written by the CFO and VP R&D and to be annually approved by Gravyty's management.

26.4. The VP R&D is to adjust the nature of backup procedures for each computer system, depending on the availability required from the system.

27. Compliance

27.1. Compliance with corporate information security requirements

27.1.1. Gravyty's management is required to comply with basic requirements for information security and is to operate strictly to implement this compliance.

27.2. Annual security review

27.2.1. Gravyty must conduct an annual security audit ("Audit") by a qualified and competent third-party external auditor.

27.2.2. The Audit must test the following service domains:

- Application architecture security analysis: check the system
- Implementation from a secure development aspect
- Application assessment: scanning the application using tools to discover vulnerabilities.
- External penetration: penetration attempts from the Internet to the web application environment
- Database assessment: checking database-related security
- System hardening: scanning the environment's servers.

27.2.3 The audit is to conform to the following web standards:

- CIS – Center for Internet Security: https://www.cisecurity.org/
- OWASP – Open Web Application Security Project: https://www.owasp.org/

28. Data protection and privacy

28.1. Gravyty is compliant with UK data protection legislation, the Data Protection Act of 2018 (DPA 2018), and with effect from May

25, 2018, EU General Data Protection Regulation (Regulation (EU) 2016/679) or GDPR.

28.2. Gravyty is registered as a Data Controller with the UK regulatory body, the Information Commissioner's Office (ICO), with the registration number Z2240223. Gravyty's entry on the ICO Register can be found here: https://ico.org.uk/ESDWebPages/Entry/Z2240223.

28.3. Gravyty's formal Data Protection and Privacy Policy covers all matters relating to data protection and privacy and reference shall be made to it as necessary.