goodweek

INFORMATION SECURITY POLICY

V1.2

The owner of this policy is Kevin Abrantes, CTO

VERSION	STAKEHOLDER	NAME	DATE	CONTENT
1.0	Author	K. Abrantes	Dec. 9, 2025	
	Review	V. Laffite	Dec. 11, 2025	
		D. Masson	Dec. 13, 2025	
	Validation	G. Nominé	Dec. 15, 2025	
1.1	Author	K. Abrantes	Mar.10, 2026	Add Cryptography section + Timeline to remediate vulnerabilities + change Title Kevin Abrantès
	Review	V. Laffite	Mar.11, 2026	
		D. Masson	Mar.12, 2026	
	Validation	G. Nominé	Mar.12, 2026	
1.2	Author	K. Abrantes	Oct.1, 2026	Hosting moved to AWS: Network security section updated (SSO and Systems Manager access) + change Title Kevin Abrantès
	Review	V. Laffite D. Masson	Oct.2, 2026 Oct.2, 2026	
	Validation	G. Nominé	Oct.5, 2026	

Goodweek Security Contacts

CEO: Guillaume Nominé - guillaume.nomine@goodweek.com

CTO (Head of Security): Kevin Abrantes – kevin.abrantes@goodweek.com

DPO: David Masson - privacy@goodweek.com / david.masson@goodweek.com

To report a security incident: security@goodweek.com

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all Goodweek employees and external providers/contractors.

All Goodweek employees and external providers/contractors must read this document in its entirety and sign the form confirming they have read and understand this policy fully.

This document will be reviewed and updated by management of Goodweek on an annual basis or when relevant to include newly developed security standards into the policy and distribute it to all employees and external providers/contractors, as freelance for example, as applicable. For the purpose of this Policy, the above-mentioned related partners, external providers as contractors, etc. are deemed to be Goodweek employees as it relates to security and compliance.

2. Information Security Policy

Goodweek commits to protect any information about its clients or shared with them and confidential information of Goodweek including know-how (together the "**Data**") from any not authorized third parties, Data being confidential by nature.

To this end management is committed to maintaining a secure environment.

Employees handling Data should ensure the following:

- Handle any Data including Company and client information in a manner that fits with their sensitivity;
- Limit personal use of Goodweek information and telecommunication systems and ensure it doesn't interfere with their job performance;
- Do not use e-mail, internet and other company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorized;
- Protect Data in any circumstance;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorized software or hardware, including modems and wireless access unless explicit management approval;
- Always leave desks clear of Data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response – Making sure to find out who this is.

We each have a responsibility for ensuring our company's systems and Data are protected from unauthorized access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your manager.

3. Acceptable Use Policy

The Management's intentions are not to impose restrictions that are contrary to Goodweek's established culture of openness, trust and integrity.

Management is committed to protecting the employees, partners and Goodweek from illegal or damaging actions by individuals, either knowingly or unknowingly. Goodweek will maintain an approved list of technologies and devices and personnel with access to such devices.

- Each employee or external provider is responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees and external providers should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees and external providers should take all necessary steps to prevent unauthorized access to Data (that includes personal data, as a reminder).
- Employees and external providers should ensure that technologies should be used and setup in acceptable network locations
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations, whether belonging to Goodweek or not, should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees or/and external providers from a company email address and or using the brand Goodweek, to newsgroups must be approved before posting by Goodweek and should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Goodweek, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment or any contract with related contract partners. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

5. Protected stored data

All Data stored and handled by Goodweek and its employees must be securely protected against unauthorized use at all times. Any Data that is no longer required by Goodweek for business reasons must be discarded in a secure and irrecoverable manner.

6. Information Classification

Data and media containing Data must always be labelled to indicate sensitivity level.

- Data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or Data that would cause severe damage to Goodweek if disclosed or modified. Data (which is confidential) includes, but are not limited to, personal, customer, activation codes, trade secrets, know-how, information under a Non Disclosure Agreement, etc.

- Internal Use Data might include information that the data owner feels should be protected to prevent unauthorized disclosure;
- Public data is information that may be freely disseminated.

7. Physical security

Access to Data in both hard and soft media format must be physically restricted to prevent unauthorized individuals from accessing any Data.

- Employees and external providers are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees and external providers should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees and external providers should take all necessary steps to prevent unauthorized access to Data.
- Employees and external providers should ensure that technologies should be used and setup in acceptable network locations
- An updated list of devices should be maintained.
- The list should include make, model and location of the device, including identification information of the device.
- Personnel using the devices should verify the identity of any third-party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behavior and indications of tampering of the devices to the appropriate personnel.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, disks, USB keys, back-up devices, hard drives, etc.
- Media containing Data including customer information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold Data. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where Data is accessible.
- Strict control is maintained over the external or internal distribution of any media containing Data.
- Strict control is maintained over the storage and accessibility of media.
- All computers that store Data must have a password protected screensaver enabled to prevent unauthorized use.

8. Protect data in transit

All Data must be protected securely if it is to be transported physically or electronically.

- If there is a business justification to send Data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, SSL, TLS, IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing Data to another location must be authorized by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

9. Cryptography

- Getpulse Inc. shall evaluate the risks inherent in processing and storing data, and shall implement cryptographic controls to mitigate those risks where deemed appropriate. Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented. All encryption shall be performed in accordance with industry standards, including NIST SP 800-57.

- Access to keys and secrets shall be tightly controlled in accordance with the Access Control Policy.

- The following table details Getpulse Inc.'s approved encryption algorithms:

Domain	Key Type	Algorithm	Key Length	Max Expiration
Web Certificate	RSA or ECC with SHA2+ signature	RSA or ECC with SHA2+ signature	2048 bit or greater/RSA, 256bit or greater/ECC	Up to 1 year
Web Cipher (TLS)	Asymmetric Encryption	Ciphers of B or greater grade on SSL Labs Rating	Varies	N/A
Confidential Data at Rest	Symmetric Encryption	AES	256 bit	1 Year
Passwords	One-way Hash	Bcrypt, PBKDF2, or scrypt, Argon2	256 bit+10K Stretch. Include unique cryptographic salt+pepper	N/A
Endpoint Storage (SSD/HDD)	Symmetric Encryption	AES	128 or 256 bit	N/A

- Requests for an exception to this practice must be submitted to the CTO for approval.

- A documented exception is required prior to moving, copying, or storing customer or company confidential data on any media or removable device; all portable devices and removable media containing sensitive data must be encrypted using approved standards and mechanisms.

10. Disposal of Stored data

- All Data must be securely disposed of when no longer required by Goodweek, regardless of the media or application type on which it is stored.
- All hard copies of personal data must be manually destroyed when no longer required and based on the Data Retention Policy's provisions.

11. Security awareness and procedures

The policies and procedures outlined below must be incorporated into the company's practice to maintain a high level of security awareness.

- The protection of Data demands annual training of all employees and contractors on security fundamentals.
- Distribute this security policy document to all company employees & freelancers to read. It is required that all employees & freelancers confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- Company security policies must be reviewed annually and updated as needed.

12. Network security

- Goodweek operates its production environment using third-party cloud platforms (AWS managed services) and does not operate any self-managed servers or corporate (office) network.
- AWS is considered subservice organization for the system; it operates security controls for the underlying infrastructure and platform network, while Goodweek is responsible for secure configuration and access management for the services it uses.
- Administrative access to AWS goes through AWS IAM Identity Center (single sign-on), is restricted to authorized personnel, is granted based on least privilege, and requires multi-factor authentication (MFA).
- Where SSH is used (e.g., for platform interactions), Goodweek uses key-based authentication and does not use passwords for SSH authentication.
- Goodweek minimizes public exposure by only enabling required inbound connectivity for the application and by configuring cloud resources to prevent unintended public access (e.g., S3 Block Public Access unless a documented exception exists).
- Goodweek monitors security-relevant events in its cloud environment (e.g., authentication activity and security configuration changes) and follows a documented incident response process for investigation and remediation.
- Changes that may impact security posture or external exposure (e.g., IAM permissions, resource access settings, and platform access settings) are authorized, documented, and approved prior to implementation.

13. System & Password policy

- All users, including contractors and vendors with access to Goodweek systems, are responsible for taking appropriate steps to protect their credentials and access.
- All users must have a unique user ID; generic accounts must remain exceptional
- User access is granted based on least privilege and must be removed promptly upon termination or when no longer required.

- Administrative access to Microsoft 365 and cloud consoles requires multi-factor authentication (MFA).

Where passwords are used, the responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:

- Be as long as possible (never shorter than 8 characters).
- Not be based on any personal information.
- Not be based on any dictionary word (in any language) or a commonly used password.
- May include mixed-case letters, digits, and punctuation marks to increase uniqueness.

All administrative access uses encrypted channels (e.g., HTTPS/TLS, AWS Systems Manager and SSH where applicable); insecure remote access methods (e.g., telnet) are not permitted.

14. Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by Goodweek.
- The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- Removable media (USB, portable hard drives, etc.) should be used with caution. If such equipment must be used, they should be scanned for viruses before being used.
- Master Installations of the Antivirus software should be set up for automatic updates and periodic scans.
- End users must not be able to modify and any settings or alter the antivirus software
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

15. Patch management policy

- All Workstations, servers, software, system components etc. owned by Goodweek must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Wherever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches must be installed within one month of release from the respective vendor and must follow the process in accordance with change control process.
- Any exceptions to this process must be documented.

16. Remote access policy

- Remote access to Goodweek systems (including cloud consoles and administrative tooling) is restricted to authorized users and must be protected using multi-factor authentication (MFA) or key-based authentication where applicable.
- Remote access privileges are granted based on least privilege and are approved prior to provisioning.
- Third-party (vendor) remote access is granted only for a documented business purpose, is limited to the minimum scope and duration necessary, and is removed promptly when no longer required.

- Remote access activity is logged and monitored on a regular basis, and access rights (including vendor access) are reviewed periodically to confirm ongoing business need.

17. Vulnerability Management policy & penetration testing

- All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices
- Timeline to remediate vulnerabilities:
  - Critical and High severity vulnerabilities must be remediated and deployed to production within one month of detection, unless a documented risk acceptance is approved by the CTO.
  - Medium and Low severity vulnerabilities are grouped and addressed during regular maintenance windows, according to business priorities.
  - If a vulnerability cannot be remediated within the defined timeframe, the Tech Lead documents the reason, compensating controls (if any), and a target remediation date in the Jira tracking ticket, and seeks approval from the CTO.

- External intrusion tests will be performed remotely from the supplier's premises.
- If an incident occurs during the execution of the tests that have an impact on the systems or services of the organization, the incident should be brought immediately to the attention of those responsible for incident management
- The scope of the test should include, at least, all systems and applications that are part of the core Goodweek production systems.
- Technical tests must follow the OSSTMM methodology. Tests must be conducted at network, system and application level and must ensure that at least identifies any vulnerabilities documented by OWASP
- For all findings or vulnerabilities identified during the tests, carried out will be generated and documented sufficient evidence to prove the existence of the same.
- As a result of tests performed should generate a document containing at least the following sections:
  - Executive Summary
  - Methodology
  - Identified vulnerabilities + evidences
  - Recommendations for correcting vulnerabilities
  - Conclusions

18. Configuration standards

- Information systems that process transmit or store Data must be configured in accordance with the applicable standard for that class of device or system.
- All network device configurations must adhere to Goodweek required standards before being placed on the network.
- Before being deployed into production, a system must be certified to meet the applicable configuration standard.
- Updates to network device operating system and/or configuration settings that fall under Goodweek standards are announced by the Information security responsible. Updates must be applied within the time frame identified by the Information security responsible.
- Administrators of network devices that do not adhere to Goodweek standards (as identified via a previous exception) must document and follow a review process of announced vendor updates to

operating system and/or configuration settings. This process must include a review schedule, risk analysis method and update method.
- All network device configurations must be checked annually against the configuration boilerplate to ensure the configuration continues to meet required standards.
- Where possible, network configuration management software will be used to automate the process of confirming adherence to the boilerplate configuration.
-

19. Change control process

- A change management policy is enforced and reviewed every year.
- This Policy ensures that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner.
- This Policy includes management responsibilities and procedures.
- All change requests shall be logged whether approved or rejected on a standardized and central system. The approval of all change requests and the results thereof shall be documented.
- A risk assessment shall be performed for all changes and dependent on the outcome, an impact assessment should be performed.
- Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.
- All changes shall be approved prior to implementation.
- All users, significantly affected by a change, shall be notified of the change.
- Implementation will only be undertaken after appropriate testing and approval by stakeholders.
- Information resources documentation shall be updated on the completion of each change.
- Specific procedures to ensure the proper control, authorization, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.
- All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

20. Audit & Log review

- Goodweek collects and retains audit logs and security-relevant logs for systems within the production environment, focusing on events needed to support security monitoring, incident investigation, and accountability.
- At a minimum, logs include authentication and authorization events, privileged/admin activity, and changes to security-relevant configurations for the production environment and cloud services.
- Access to logs is restricted to authorized personnel based on least privilege, and logs are protected against unauthorized access and deletion.
- Automated alerting is configured for suspicious or anomalous activity, and alerts are reviewed and investigated in accordance with the incident response process.
- Logs are retained for at least 90 days in readily accessible storage and at least 12 months in archived storage (or longer if required by contractual or legal obligations).

21. Secure Application development / Use of Generative AI

The Secure Application development policy is a plan of action to guide developers' decisions and actions during the software development lifecycle (**SDLC**) to ensure software security. This policy aims to be language and platform independent so that it is applicable across all software development projects.

The adherence to and use of Secure Application Development Coding Policy is a requirement for all software development on Goodweek information technology systems and trusted contractor sites processing Goodweek data.

Development of code shall be checked and validated with the most current versions of Goodweek Coding Standards for Secure Application Development. All code developers shall verify that their code is in compliance with the most recent and approved coding standards and guidelines.

Only validated code shall be implemented into Goodweek production environment. A review and validation ensure that code exhibits fundamental security properties to include correctness, predictability, and attack tolerance.

Application Code Developers shall:

- Ensure code meets the level of confidence that software is free from exploitable code vulnerabilities, regardless of whether they are already designed into the software or inserted later in its life cycle.
- Ensure code provides predictable execution or justifiable confidence and that the software, when executed, will provide security functionality as intended.
- Coding techniques must address injection flaws particularly SQL injection, buffer overflow vulnerabilities, cross site scripting vulnerabilities, improper access control (insecure direct object reference, failure to restrict URL access, directory traversal etc.,), cross site request forgery (CSRF), broken authentication and session management.
- Never trust incoming data to the system, apply checks to this data.
- Never rely on the client to store sensitive data no matter how trivial.
- Disable Error messages that return any information to the user.
- Use environment variables prudently and always check boundaries and buffers.
- Applications must validate input to ensure they are well-formed and meaningful.

The use of any Generative AI tool for coding is subject (i) to the present Policy on SDLC and (ii) to approval of Goodweek CTO (or his/her deputy) prior to the development of any related software development. In any event, developers shall comply with the following requisites when using any generative AI tool:

- Don't include Data and any Goodweek's and Client's proprietary, confidential or sensitive information (including the names/brands of clients) in the input or training data.
- Do obtain a prior approval from their manager (and if not possible the CTO)
  - Must not input any Data into Generative AI prompts or training datasets.
  - Generative AI outputs must be reviewed by a qualified human before use in production ("human-in-the-loop"), and developers remain accountable for the final code and design decisions.
  - Use of Generative AI must not be intended to recreate third-party proprietary work, and developers must respect applicable licenses and intellectual property rights.

22. Incident Response Plan

A specific Incident Response Policy is stored in the Goodweek documentation SharePoint. This policy is updated every year. The way we manage security incidents is reminded in the security awareness training each employee/external consultant must attend every year.

The way to report an incident should be known by all employees and external providers. Use the address: **security@goodweek.com**

Emergency Security Incident Response Team:

- **CTO: Kevin Abrantes**
- **CEO: Guillaume Nominé**
- **Personal Data Contact / CLO: David Masson**

23. Roles & responsibilities

Goodweek **CTO** is responsible for overseeing all aspects of information security, including but not limited to:

- Creating and distributing security policies and procedures.
- Monitoring and analyzing security alerts and distributing information to appropriate personnel.
- Creating and distributing security incident response and escalation procedures

Super admins shall:

- administer user accounts and review access rights at least annually

The **COO** is in charge of:

- Maintaining a list of critical providers.
- Ensuring there is a process for engaging critical service providers including proper checks prior to engagement.
- Doing a risk assessment every year and reviewing it regularly to consider some changes in the context of the company, in technology and new threats

The COO & HR lead are responsible for tracking employee participation in the security awareness program, including:

- Facilitating participation upon hire and at least annually.
- Ensuring that employees acknowledge in writing at least annually that they have read and understand Goodweek's information security policy.

CLO will ensure that for contracts, security requirements are implemented as stated in the present Security Policy.

DPO is in charge of:

- Ensures GDPR compliance of information security measures related to personal data.
- Advises on security controls impacting personal data (access control, encryption, incident management).
- Supports risk assessments and DPIAs to evaluate privacy impacts.
- Leads personal data breach governance, including regulatory notification.

24. Access control policy

Access to Goodweek systems and services is provided through individual user accounts (SSO where available). Shared or generic accounts are prohibited unless formally approved as an exception with compensating controls and time limits.

- Access rights are granted based on least privilege and need-to-know, aligned to job responsibilities.
- Privileged access is restricted, controlled, and granted only with documented approval by the system owner (or designated control owner).
- All access requires authentication and authorization prior to granting access to systems or Data.
- User access is revoked promptly upon termination or when access is no longer required.
- System owners (or delegated owners) perform periodic access reviews (at least annually) to confirm users' access remains appropriate, including privileged and third-party access where applicable.

25. Wireless policy

A quarterly test should be run to discover any wireless access points connected to Goodweek network;
Any devices which support wireless communication remain disabled or decommissioned for unauthorized wireless stations.

If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the Engineering team has the authorization to stop, cease, shut down, and remove the offending device immediately.

*
* *

Appendix A – Agreement to Comply with Information Security Policy

_____
External Provider's or Employee's Name:
_____

I have read and understand this policy, and I understand how it impacts my job.
As a condition of continued employment/contract, I agree to abide by the policy and other requirements found in Goodweek security policy. I understand that noncompliance will be cause for disciplinary action up to and including dismissal. I also agree to promptly report all violations or suspected violations of information security policies.

Date:
_____
Signature