An Overview of GainPlus Security Policies

GainPlus Solutions

+66 2 401 9255

16th Floor, Sitthivorakit Building, 5 Soi Pipat, Silom Bangkok 10500

Table of Contents

1.1. Our Commitment to our Users *3*
1.2. SaaS Platform *3*
1.3. SaaS Architecture *3*
1.4. Data Access *3*
GainPlus HTTPS port 443 4
1.5. Our Infrastructure *5*
Our Cloud Service Provider 5
1.6. System and Network *5*
1.7. Payment Processing *5*
1.8. Data in Transit *5*
Data Retention *6*
What happens to your data if you leave GainPlus? 6
1.9. Data Breach Notification *6*
Lawful Purposes 6
Data Minimisation 6
Accuracy 6
Data Retention 7
Security 7
Breach 7
1.10. Integrations *7*
1.11. Vulnerability management *7*
Preventative Maintenance 7
End Point Protection 8
Responsible Disclosure 8
1.12. Workflows *8*
Software Development 8
Software Testing 8
1.13. Risk Management *8*
1.14. Information Security policies *9*
1.15. Personal Data *9*
Compliance and certifications 9
1.16. Roadmap *9*

1.1. Our Commitment to our Users

GainPlus management is committed to the continual improvement of the information security of our organisation. Our practices follow industry-set baselines and best practices. To ensure the reliability and stability of our applications and services, we meet the Center for Internet Security (CIS) benchmark for relevant servers. We follow recommendations from the National Institute of Standards and Technology (NIST) regarding security controls such as cryptography, processes such as change management, and guidelines such as password construction. Part of our internal exercise to ensure the platform stays resilient and a demonstration of our resolve and credibility to provide a secure solution to the market as we continue our growth, we regularly (monthly) conduct Penetration Testing to subject our public-facing applications against OWASP Top 10 and SANS CWE/25 web application standards.

1.2. SaaS Platform

The GainPlus application is an all-cloud HR management SaaS platform available in both web and mobile formats (iOS and Android). Users access our services and content through modern web-browsers on an internet-connected desktop or smartphone. We do not maintain any physical servers or storage devices to run our applications. Our services are built on a fully cloud infrastructure provided by Digital Ocean in Singapore. We employ redundancy measures to ensure high availability across our platform. This helps us achieve our committed Service Level Agreements (SLAs).

1.3. SaaS Architecture

We are using both multi-tenancy and multi-instance approaches. For white-labeling partnership, the isolation of data and resources that clearly identifies customer data is implemented (multi-instance). Else, only logical (code logic) isolation is implemented across the SaaS platform (multi-tenancy).

1.4. Data Access

Depending on company preferences, users can use the SAML SSO service provided by Google, Okta or Microsoft to login to their accounts. The traditional username and password credential combination is also available. User credentials encrypted and transmitted securely via TLS.

Role-based access control (RBAC): RBAC method is used to control access to the system based on individual user roles. By implementing the RBAC method, it is easier to manage the permission to the user based on the roles and organisation assigned to them. For example, employee data can only be accessed by an assigned administrator with specific roles. The allowed roles are implemented in a whitelisting approach before accessing requested resources.

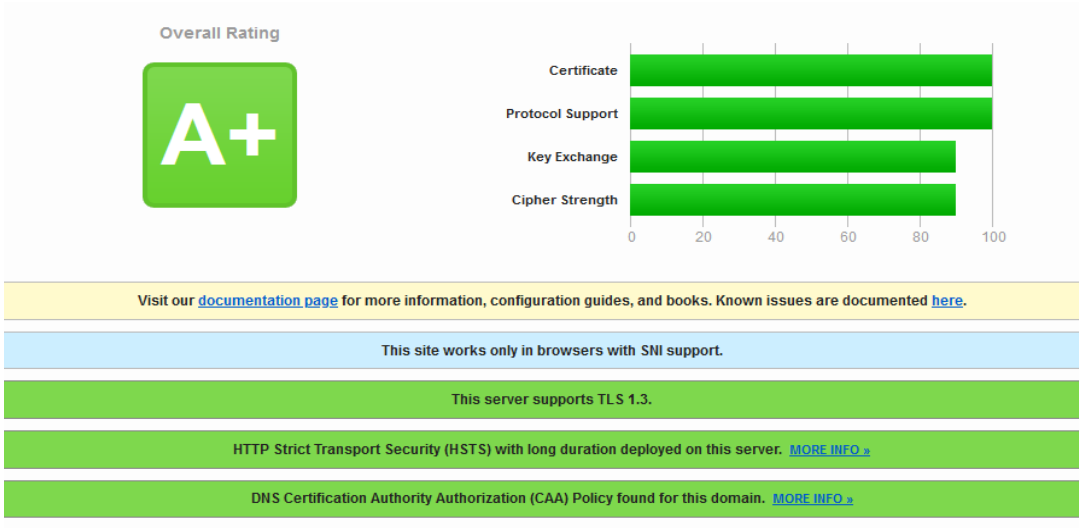
GainPlus HTTPS port 443

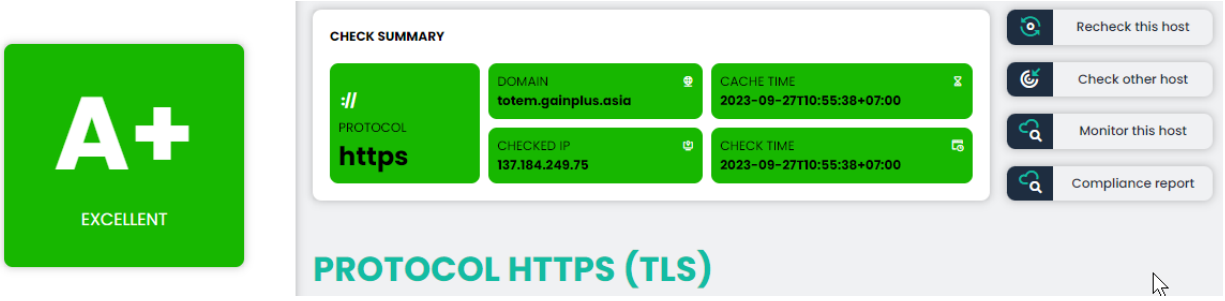
The HTTPS port on the Gainplus Totem server will only support TLS 1.2 and above, and makes use of only 8 cypher suites:

Cipher Suites
TLS 1.3
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA)
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA)
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA)

TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp521r1 (eq. 15360 bits RSA)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp521r1 (eq. 15360 bits RSA)
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp521r1 (eq. 15360 bits RSA)

Note that these cipher suites are all perfect forward secrecy (PFS) suites and are considered cryptographically secure as of the writing of this document. When the server is deployed on the Internet, https://ssllabs.com gives the server an A+ rating with no known vulnerabilities and no weak ciphers detected.





1.5. Our Infrastructure

Our Cloud Service Provider

We use **DigitalOcean** as our Service Providers in Singapore.
We use Akamai as our backup Service Provider in Singapore.

DigitalOcean is AICPA SOC 2 Type II and SOC 3 Type II certified. By achieving compliance with this globally recognized information security controls framework, audited by our independent auditor (Schellman & Company LLC), DigitalOcean has demonstrated a commitment to protecting sensitive customer and company information.

1.6. System and Network

Our infrastructure is contained within our access-controlled cloud servers which provides total isolation. Network segmentation is achieved by dividing our cloud servers into public and private subnet layers. We maintain separate development, staging and production accounts for each layer of our service. Only shared services have access to our staging and production environments. A process is in place for requesting and approving remote connections to servers. The "least privilege" model ensures that only users who need access in the fulfillment of their duties and responsibilities are granted the appropriate rights and permissions. Privileged access is performed over secure channels (eg over encrypted network connections using SSH). Activities performed using shared and privileged accounts are monitored. Access control (ie security groups, users, roles, and permissions) is reviewed regularly. Our public-facing web applications and APIs are also protected by firewalls, cloud-based web application and API protection (WAAP) service which provides a combination of distributed denial of service (DDoS) protection, bot mitigation, API protection and a web application firewall (WAF). We follow the following standards as our server security baselines: NIST Special Publication 800-123: Guide to General Server Security, CIS-20 Controls for Implementation Group 2, and AWS Security Best Practices.

1.7. Payment Processing

We do not store any PCI information in our databases and logs.

1.8. Data Encryption

Data from users to our services are over a secure HTTP (HTTPS) connection and encrypted end-to-end using SHA256 ECDSA for signing and SHA256 RSA for compatibility. We only allow HTTPS connections from visitors supporting TLS v1.2 and above. These protocols offer modern authenticated encryption (also known as AEAD) for added security.

Databases are encrypted at rest using industry standard AES-256. Additionally, we also encrypt backups using the AES-256 encryption algorithm.

Data Retention

We retain data for as long as necessary to fulfill the purposes for which we collected it. This also includes satisfying any legal, accounting, or reporting requirements, to establish or defend legal claims, or for fraud prevention purposes. Our policies have defined a retention period of one year but not more than seven years. This period allows for analysis and investigations should the need arise.

What happens to your data if you leave GainPlus?

If a client terminates or cancels their subscription with us, they can request for a deletion of their account. However, the data from backups and logs will be retained according to our data retention policies. A client may request a copy of their data, but this should be made before requesting for the deletion of their account.

1.9. Data Breach Notification

Our info sec policies include a data breach plan included our Privacy Policy for Individuals. Customers and affected parties will be notified as soon as reasonable. Any parties affected will be contacted through the company information provided or through published communication channels.

Lawful Purposes

- All data processed by the organisation must be done on one of the following lawful bases: consent, deemed consent (notification, legitimate interest, business improvement and research) , contract, legal obligation, vital interests or public task.
- Reliance of the organisation in the collection, use and disclosure of personal data for any of the purposes in which the consent is deemed should undergo risk assessment. This assessment shall be documented. When necessary and required by law, reliance on this consent shall be made available to the users.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent, except when it falls under deemed consent by notification, shall be documented.
- Where communications are sent to individuals based on their consent, the option for the individual to withdraw their consent should be clearly available and systems should be in place to ensure such withdrawal is reflected accurately in the GainPlus systems.

Data Minimisation

- The organisation shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

- The organisation shall take reasonable steps to ensure personal data is accurate.
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Data Retention

- To ensure that personal data is kept for no longer than necessary, the organisation shall put in place a data retention policy for each area in which personal data is processed and review this process annually.
- The data retention policy shall consider what data should be retained, for how long, and why.

Security

- The organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal data is deleted or anonymised - this should be done safely such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

Breach

- In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the appropriate regulatory body.

1.10. Integrations

Indirect or third party access refers to a situation in which our customer data is viewed or used by a third-party application or custom interface. Authorised third-party integrations have legitimate business cases as part of the company's offering of services such as payroll and staffing services, software, products and support. Our third-party integrations, such as Xero, are accessed via our external API. OAuth tokens or any customer-identifying information are not exposed within our applications nor shared with other parties. All integrations are accomplished using oAuth v2.0. "Bearer tokens" and not credentials (user and password) are used to authenticate each request. Each request is protected in transit through HTTPS.

1.11. Vulnerability management

Preventative Maintenance

The most recent and critical security patches must be installed on the system as soon as practical and reasonable. Immediate application of security patches is ideal unless this interferes with business requirements where a reasonable expectation of delay is justified. Regular preventive maintenance (security and/or system patches) will also be carried out once a month.

End Point Protection

End-point protection is another layer of security protection for our company assets (data and resources) against malicious attacks, ransomware and viruses. All end-points that are connected to internal networks via remote access technologies or personal workstations (BYOD) that access company resources use the most up-to-date anti-virus software.

Responsible Disclosure

A publicly-available page that outlines how independent security researchers, who understand the severity of the risk, can disclose security vulnerabilities found on our products and services. Our responsible disclosure page is located here.

1.12. Workflows

Software Development

We adopt the best of agile practices and we continue to improve the way we work by constantly reviewing the way we work. Agile teams select the amount of work possible to be done based on their availability. Agile iterative development means that the team itself may decide what it is able to do based on their capabilities and experience from the previous iteration. The Engineering Team runs a very tight ship. Workflows are almost clearly outlined and followed by every single member of the Engineering Team and reviewed almost every month for improvements.

Software Testing

In an Agile environment, the Engineering, Product and Quality Assurance Team, work collaboratively to make improvements on an ongoing basis. We embrace a shared responsibility in ensuring we deliver a high-quality end product and service. Our software testing processes aim to deliver consistent results through a set of standardised procedures to ensure that the product design does not only meet the requirements and specifications of our customers but is free from bugs, errors, vulnerabilities and other defects. We minimize the risk of defects while maximizing end-user experience by incorporating software and quality assurance testing throughout our entire engineering process. Our testing methods utilise both manual and automated processes.

1.13. Risk Management

The core of our information security framework is geared toward managing the risks that affect confidentiality, integrity and availability of our application and services. We follow the ISO 27001 recommendations for risk management. To determine our set of basic security controls - we follow the 20 prioritised set of actions from the Center for Information Security. CIS-20 collectively form a defence-in-depth set of best practices from security researchers all over the world that mitigate the most common attacks against systems and networks. Thus, CIS-20 provides us with the sufficient basis to kickstart our information security framework.

1.14. Information Security policies

The information security framework contains a list of documents and policies that defines our cybersecurity program. These documents are the cornerstone of the information security framework that reflects our security perspective and the management's strategy for securing data and information. How do we maintain accuracy in our records and documents?Information security-related records and documents are protected against unauthorised changes or deletion according to the Access Control Policy. Logs and audit trails are immutable and system-generated. Request for access to information follow the Information Classification and Handling

1.15. Personal Data

GainPlus Solutions Limited takes the privacy of your personal data very seriously, and we do so in accordance with the General Data Protection Regulations (GDPR), the Data Protection Act 2018 and Privacy and Electronic Privacy Regulations (PECR) and any other applicable legislation. We act as a data Controller for the personal data we process about our employees; our customers and suppliers (current and prospective); our visitors; enquirers and those who engage with our website and directly with us
We act as a data Processor in these circumstances (not the Controller). If your data is managed by one of our customers, then the data Controller for your information will be that organisation (eg your employer) and you should refer to their privacy information and notices.

Compliance and certifications

As an organisation, the ISO 27001 compliance is in the road-map.

1.16. Roadmap

We are moving into integrating ISO 27001:2013 controls into our information security processes with a special focus on effective risk management. By implementing these controls, we secure our employee and customer data, we increase resilience to cyber attacks and reduce the costs associated with information security by eliminating redundancies and streamlining processes.