Information Technology FAQs

Exported on 14/12/2023

Unit 6, 1 Metier Linkway, Birtinya, QLD 4575 | Australia
Phone +61 7 3186 0203 | sales@greaseboss.com.au | www.greaseboss.io

1 Organisational Information Security

Do you have an Information Security policy, standards and procedures in place?
Yes - GreaseBoss Information Security Policy

Are your Information Security Policy, Standards, and Procedures maintained and reviewed at least on a periodic basis?
As per the policy, a review is conducted regularly following organisation or legislative changes or, as a minimum every (12) months.

What data is stored?
The data stored on the GreaseBoss system is not sensitive data. The only data stored/transmitted is machinery greasing data (i.e. for a specific grease point - the grease type, required volume and schedule for greasing).

The "grease event" data (the IoT packet data) consists of:

- RFID code of grease point
- grease volume dispensed
- time and date of grease dispensed
- all asset identifiers are transferred via GUID's

Do you have any independent security attestation like ISO 27001, PCI, SOC-2?
GreaseBoss is currently working towards obtaining SOC-2 and ISO 27001 accreditations.

Is there an Information Security function responsible for security-related concerns?
Head of Software and CTO are responsible for Information Security.

Is there a security awareness training program? Does it include a mandatory training session for new hires and periodic training for existing employees?
A security awareness training program is currently being rolled out with GreaseBoss and to be completed by all GreaseBoss employees

Are there confidentiality or non-disclosure agreement(s) with employees and third parties reflecting the organisation's needs for the protection of information?
Non-disclosure agreement(s) are signed by all employees, contractors and consultants.

Do you review and revoke logical and physical access rights from all systems upon termination (voluntary and involuntary), transfer or other similar events on or before the effective termination date?
Upon termination logical and physical access rights are removed to GreaseBoss systems.

Do you have cyber insurance?
Not currently, GreaseBoss is in the process of getting this organised.

What due diligence is performed on the upstream and downstream service providers you rely on for end-to-end delivery of your product or service?
Service providers must conform to the GreaseBoss Cloud Policy; only authorised cloud providers (AWS, Azure and GCP) can be used.

Is your platform or service externally audited?
GreaseBoss is currently preparing to obtain SOC-2 and ISO 27001 accreditations which will require our platform and service to be externally audited.

Please disclose the locations where you store, back-up, process and access information.
All data and services reside within Australia by default, customers requiring data to reside in their own region may do so but will require their own instance of the services to be running.

GreaseCloud uses AWS, Region Code: ap-southeast-2 - Asia Pacific (Sydney)

Is the data encrypted?
All data is stored using MongoDB (NoSQL), cloud-based installation utilise MongoDB Atlas which by default implements the following:
- Encryption at Rest and Encryption in Transit
- Network Isolation
- Role-based access management

Is Intrusion Protection (IPS) or Intrusion Detection (IDS) Systems deployed to protect the systems or services being provided?

Yes, GreaseCloud utilises AWS Web Application Firewall for Intruder Detection and Intruder Protection.

2 Physical and Environmental Security

Do you have a Physical & Environmental Security Policy in place?
As per the GreaseBoss Cloud Security Policy:

GreaseBoss adopts the shared responsibility model, whereby the cloud provider is responsible for protecting the infrastructure (hardware, software, networking and facilities) that runs all of the services. GreaseBoss operates all its systems within the cloud, therefore has no physical servers on-site.

3 Data Communication and Operation Security

Are all of your company's applicable hardware systems, including servers, desktops, and laptops, up-to-date with current versions of industry-accepted, preventative software which addresses, but is not limited to, antivirus, Trojans/worms, spyware, root-kits, as well as other forms of malicious software?Yes, as per the GreaseBoss Patch and Vulnerability Management Policy.

Do you perform routine vulnerability assessments on your platform or service? If so, how often are they performed?
Yes, the following is used:

- **AWS Inspector**
  - Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure
- **Intruder.io**
  - Online vulnerability scanner to detect cyber security weaknesses.
  - Emerging threat scans are automatically performed when new vulnerabilities are identified.
  - Weekly vulnerability scans are performed.

What is your policy for fixing issues identified by your vulnerability scanners?

- Critical Severity within 7 days
- High Severity within 30 days
- Medium Severity within 60 days
- Low Severity within 120 days

Are penetration tests performed by a qualified independent third-party on your platform or service? If so, how often are they performed?
We are looking to undertake an independent third-party penetration test within the next 6 months.

Our plan is to conduct an independent third-party penetration test at least once per year or as required based on new threats and vulnerabilities.

4 Cloud Security

Is multifactor authentication (MFA) available for cloud administrative session?
GreaseCloud supports Multi-Factor Authentication (MFA).

GreaseCloud authentication and authorisation is carried out using OAuth 2.x and OpenID Connect protocols. All access to the GreaseCloud, whether it be a web browser, mobile device or a GreaseBoss Head Unit use this mechanism. The identity server used by GreaseCloud is officially certified by the OpenID Foundation.

5 Access Control

Is there an Access Control Policy in place? If yes, does the policy outline the principle of least privileged and need to know basis?
Yes - GreaseBoss Information Security Policy

Is there a password policy in place? If yes, whether password policy is enforced while creating new users?
Yes - GreaseBoss Password Policy

6 Information Security Incident Management

Do you have a formal privacy incident communication procedure, integrated with the security incident response and escalation procedures to be executed in the event of unauthorised disclosure or breach?
Yes - GreaseBoss Incident and Response Process

7 Information Security for Business Continuity and Disaster Recovery

Do you have business recovery plan/technology recovery plan for the services provided?Yes - GreaseBoss Cloud Disaster Recovery Policy and Plan

Are your business/technology recovery plans updated, reviewed, and approved on a periodic basis or when significant operational changes are implemented?
As per the policy, a review is conducted regularly following organisation or legislative changes or, as a minimum every (12) months.

8 Installation

What is the default installation?
GreaseCloud is offered as a multi-tenant solution using AWS, whereby infrastructure and data resides in Australia as per our Cloud Security Policy. Access to site data is strictly controlled by our authentication and authorisation mechanisms, and users have to be granted permission to access the data by a site administrator.

What other installation options are available?
GreaseBoss can also offer the following installation options:

- Public Cloud - Single Tenant
  - GreaseCloud can be set-up as a dedicated instance for your organisation.
- Private Cloud
  - GreaseCloud can be set-up to run in your own cloud infrastructure.
- On-Premise
  - GreaseCloud can be set-up to run on your own servers.

9 Software Development and Maintenance

Do we develop the software or engage a third-party to develop the software for the cloud service
GreaseBoss develops the software for the cloud service and head units.

Do you use industry standards to build in security for your System/Software Development Lifecycle
We use the Australian Cyber Security Centre Guidelines (https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-software-development) and Microsoft Security Development Lifecycle (https://www.microsoft.com/en-us/securityengineering/sdl/practices) as part of our secure software development process.

In summary:

- We have segregated development, staging and production environments including associated data.
- We use secure-by-design, with security measures applied at multiple layers, for example:
    - We use AWS Web Application Firewall
    - Identity Service to handle authentication and authorisation, runs independent of our backend as an additional layer of separation
    - API Gateway has authentication and CORS policies
    - Each micro-service has authentication and CORS policies
    - HTTPS secure by TLS by default.
    - Web browser-based security controls, such as Content-Security-Policy, HSTS and X-Frame-Options
    - Adopt databases that support the latest security measures such as encryption at rest, and in-transit etc
- Threat Modelling and Risk Assessments
- Development process
    - We adopt a Pull Request process, so code has to be approved prior to merging.
    - Static Analysis Security Testing
    - Third-Party components (both commercial and open source) are vetted to understand security vulnerabilities.
    - Use Approved Tools
    - Coding standards
- Software releases are deployed to staging and tested prior to deployment to Production
- Our vulnerability scanners (AWS Inspector, Intrudor.io etc) are continuously scanning our development, staging and production environments.
    - We have the capability to run ad-hoc scans as required, and these are carried out before and after deploying to Production.

What is your patch implementation strategy?
See Patch and Vulnerability Management Policy

Do you have change management policies in place?
Yes - GreaseBoss Change Management Policy

Are testing, QA and development environment separated from production environment? Are responsibilities segregated between different roles to ensure segregation of duties are followed throughout the SDLC process?
Testing and QA environments are separated from the production environment. User acceptance testing is carried out independent of developers.

10 Privacy

Do you have a documented privacy policy in place and does it comply with Australian Privacy Principles (APPs) / GDPR regulations?
Yes, our Privacy Policy complies to the APP/GDPR regulations.