Information Security Policy

1.0 Purpose

This policy defines client access to Information System (IS) resources, facilities and infrastructure provided by GreaseBoss, and describes the logical and physical conditions to access such items.

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

The objectives are:

- To communicate the need for access control
- To establish specific requirements for protecting against unauthorised access.
- To create an infrastructure that will foster data sharing without sacrificing security infrastructure resources.

2.0 Scope

This policy applies to:

- All Information System (IS) resources provided and supported by GreaseBoss
- All GreaseBoss systems, networks and cloud infrastructure
- All users (including employees, contractors, consultants, and authorised visitors) of the Greaseboss IS resources.
- All connections (locally and remotely) to the Greaseboss network (LAN/WAN/WIFI/VPN/Cloud)

3.0 Abbreviations and Definitions

N/A

4.0 Policy Statement

Access to information and business processes must be controlled on the bases of business and security requirements, and is subject to the GreaseBoss Information Security Policy. Adequate security must be provided to ensure both the protection and maintenance of system integrity over the information system, information and documentation at all times.

4.1 Password

Passwords are the first line of defence for our Information Systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

More detailed information regarding the use of passwords is outlined in the GreaseBoss Password Policy.

4.2 User Access

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access.

Each user must be allocated access rights and privileges to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

The criteria used for granting access privileges must be based on the principle of “least privilege” whereby authorized users will only be granted access to Information System Resources which are necessary to carry out the responsibilities of their GreaseBoss role or function.

The creation of user access accounts with special privileges such as administrators must be rigorously controlled and restricted to only those users who are responsible for the management or maintenance of the Information Systems or network. Each administrator must have a specific admin

level account, which is only used for system administrative purposes, and is kept separate from their standard user access account.

4.3 User Responsibility

It is a user's responsibility to prevent their username and password being used to gain unauthorized access to GreaseBoss systems by:

- Following the password policy statements outlined in the Password Policy.
- Ensuring that any computer they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login name and
- passwords.

4.4 Generic Accounts

The use of shared, guest, anonymous and other such generic user accounts shall be avoided where possible.

Where possible, generic accounts must have the minimum rights and privileges required to perform their role, and must not be used to access any corporate systems or stores of confidential information.

Generic access to information stored in databases is allowed only for non-interactive tasks. A non-interactive task is the one that is scheduled to run automatically or one that is triggered by a series of events. A user does not directly initiate the task, nor is a user the direct recipient of the information. This includes automatic downloads and other linkages for data transfer.

4.5 Network Access Control

Permission must be sought from GreaseBoss to use non-GreaseBoss owned computers and other personal network devices on the network.

4.6 Operating System Access Control

Access to operating systems is controlled by a secure login process. The login procedure must also be protected by :

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded
- The password characters are hidden by symbols.

4.7 Remote Access

Remote access to the GreaseBoss network can be achieved from any authorised computer.

More detailed information regarding remote access is outlined in the Remote Access Policy.

4.8 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. GreaseBoss is responsible for granting access to the information within the system. The access must:

- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (within the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating systems that could allow
- unauthorised higher levels of access.
- Be logged and auditable.

5.0 Supporting Documents

- GreaseBoss Password Policy
- GreaseBoss Remote Access Policy

6.0 References

N/A

7.0 Review

This policy will be reviewed regularly following organisational or legislative changes or, as a minimum every (12) months.

8.0 Authorisation

Name:	Tim Hall
Role:	Chief Operating Officer
Signature:	
Date:	**02/10/2021**

9.0 Revision History

Revision	Date	Description	Author	Approver
0.1	2/10/2021	First draft	James Usherwood	Tim Hall