GLOBAL MARINE | GROUP

GLOBAL MARINE GROUP

Information Technology

Information Security Policy

GMG-D-KA-00016

Table of Contents

1. INTRODUCTION

Global Marine Group recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems underpin all the company's activities, and are essential to its ability to function effectively and efficiently.

In addition, the loss or unauthorised disclosure of information has the potential to damage the company's reputation and cause financial loss.

This policy defines a framework by which Global Marine's computer systems, infrastructure and computing environment will be protected from threats whether internal, external, deliberate or accidental.

2. AIMS OF THIS POLICY

GMG is committed to protecting the security of its information and systems in order to ensure that:

- The integrity of information is maintained, so that it is accurate, up to date and 'fit for purpose'
- Information is always available to those who need it and there is no disruption to the business of GMG
- Confidentiality is not breached, so that information is accessed only by those authorised to do so
- The company meets its legal requirements, including those applicable to personal data under the Data Protection Act
- The reputation of Global Marine is safeguarded

3. POLICY SCOPE

This policy provides a framework for the management of information security throughout the company. It applies to:

- All those with access to Global Marine's information systems, including staff, personnel on GMG managed vessels and contractors
- Any systems attached to GMG's computer network and any systems supplied by the company
- All information (data) processed by GMG pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form; any communications sent to or from GMG and any company information held on systems external to GMG's network e.g. ships' computer domains
- All external parties that provide services to GMG in respect of information processing facilities and business activities

4. POLICY IMPLEMENTATION

In order to meet the aims of this Policy, GMG will aim to implement security controls that conform to best practice, as set out in the ISO/IEC 27001:2013 Information Security Management.

The following key principles will be implemented:

- All central computer systems, environments and information contained within them will be protected against unauthorised access
- Information kept within GMG systems will be managed securely, to comply with relevant data protection laws and to satisfy GMG's expectations that such assets will be managed in a professional, safe and dependable manner
- The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of the IT Department
- All users have a responsibility to report promptly, to the IT Department, any incidents which may have an IT security implication for GMG
- All breaches of information security and related incidents will be investigated by the IT Department
- Users will be required to change there account password every 42 days, there are no exceptions.

This policy will be communicated to all relevant persons, who are required to familiarise themselves with its content and comply with the requirements.

5. THE COMPUTING ENVIRONMENT

The IT Department manages, maintains and operates a range of central computing servers, systems, backup systems, and the overall network infrastructure interconnecting these systems.

The computing environment is defined as the central computing resource and network infrastructure, and all computing devices that can physically connect to it. This includes computing hardware and software, any GMG related data residing on these machines or accessible from these machines within the GMG network environment and any media such as CD-ROMs, DVD-ROMs, portable storage devices and backup tapes. This computing environment is managed and overseen by the IT Department

All temporary and permanent connections via GMG's network, laptop docking points, the Wireless network, and the Virtual Private Network (VPN) are similarly subject to the conditions of this policy.

The IT Department reserves the right to monitor, log and analyse the content of all transmissions on networks at any time deemed necessary for performance/fault diagnostics and compliance purposes.

6. ROLES AND RESPONSIBILITIES

All Staff

Information Security and the appropriate protection of information assets is the responsibility of all users. All staff are responsible for information security and remain accountable for their actions in relation to information systems. Staff shall ensure that they understand their role and responsibilities.

All staff shall:

- Safeguard hardware, software and information in their care.
- Prevent the introduction of malicious software on the organisation's IT systems.
- Ensure their password is kept secret - passwords should not be shared under any circumstances.
- Report on any suspected or actual breaches in security.

Information Security Officer

The Information Security Officer is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes. The Information Security Officer shall:

- Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.
- Provide a central point of contact for information security.
- Ensure the operational effectiveness of security controls and processes.
- Monitor and co-ordinate the operation of the Information Security Management System.
- Monitor potential and actual security breaches with appropriate security resource.

Data Protection Officer

The Data Protection Officer is responsible for ensuring that the company remains compliant at all times with GDPR, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. The Data Protection Officer shall:

- Lead on the provision of expert advice to the organisation on all matters concerning the Data Protection Act, compliance, best practice and setting and maintaining standards.
- Provide a central point of contact for the Act both internally and with external stakeholders (including the Office of the Information Commissioner).
- Communicate and promote awareness of the Act across the company.
- Lead on matters concerning individual's right to access information held by the company.

7. PHYSICAL SECURITY

Core network equipment shall be housed in a controlled and secure environment.Critical or sensitive network equipment shall be housed in an environment that has a monitored temperature and back-up power supply. Core network equipment shall be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls. Critical or sensitive network equipment shall be protected from power supply failures.

All visitors to secure network areas shall be authorised by a senior member of the technical support team prior to any visit. Only devices approved by the IT department shall connect to a physical network port at

8. ACCESS CONTROL

Access rights to the network shall be on a strict "Need to Know" basis and will be allocated on the requirements of the user's role and business need, rather than on a status basis.

Line management shall approve user access prior to access being provided by IT support. All users to the network shall have their own individual user identification and password. Users shall ensure that their password is kept secret and never shared.

Access to any network shall be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Security privileges shall be reviewed on a quarterly basis

User access rights shall, upon notification from line management, be immediately removed or reviewed for those users who have left the department or changed roles.

Access to IFS will be requested by a finance manager and approved and implemented by the IT department, this request shall be made through the "Request a new IFS user" form.

9. THIRD PARTY ACCESS CONTROL TO THE NETWORK

Third party access to the network shall be based on a formal contract that satisfies all necessary security conditions.

IT Support shall ensure that all third party access to the network is logged.

10.DATA BACKUP AND RESTORATION

The IT department shall ensure that backup copies of switch configuration and data stored on the network are taken regularly in accordance with the Backup Policy and specific system requirements.

Documented procedures for the backup process shall be produced and communicated to all relevant staff.

Documented procedures for the storage of backup tapes shall be produced and communicated to all relevant staff.

All backup tapes shall be stored securely and a copy will be stored off-site.

Documented procedures for the safe and secure disposal of backup media shall be produced and communicated to all relevant staff.

The restoration from a backup shall be tested regularly and the process documented, the restoration testing should be at least annually.

11.MALICIOUS SOFTWARE AND ANTI-VIRUS

The company shall ensure that measures are in place to detect and protect the network from viruses and other malicious software.

White listing mechanisms shall be used to help prevent malware

12.SECURITY MONITORING

The company shall ensure that the network is monitored for potential security breaches.

The company shall retain the right to access, modify or delete all data stored on or transmitted across its network. This includes data stored in personal network folders, mailboxes etc. Data of a personal nature should be stored in a folder marked or called “Private”. This does not, however, preclude access or removal of such a folder if its removal is deemed appropriate.

The company shall retain the right to disconnect or block any device connected either by physical or wireless means to the network.

The company shall retain the right to block any physical non-approved device connected to a piece of company owned equipment.

13.UNATTENDED EQUIPMENT AND CLEAR SCREEN

Users shall ensure that they protect the network from unauthorised access.

Users shall log off the network when they have finished working.

The company operates a clear screen policy that means that users shall ensure that any equipment logged on to the network must be protected (locked via 'CTRL/ALT/DEL' or shutdown) if they leave it unattended, even for a short time.

14.PASSWORD POLICIES

All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees must choose passwords that meet the following complexity requirements:

- 8 Characters Minimum
- 12 passwords remembered
- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)

In addition to meeting those requirements, employees should apply common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective.

A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization.

Employees must choose unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account.

All passwords must be changed every 42 days. This requirement will be enforced using software when possible.

If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.

Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

ADP is a vendor controlled environment and therefore password complexity or conditioning cannot be alterred, as such this is an accepted variance to the company's password policy.

IFS is limited by vendor restriction, therefore password handling does not fully comply with this password policy in respect of forcing complexity, it does however abide by the 42 day expiry, this variation that is accepted by the company.

User Account passwords are to be kept secure and are not to be shared.

If a user believe that their password has been accidentally disclosethey are required to inform the IT department immediately. Eg. Accidental password disclosure includes entering your password on a 3rd party website by mistake.

Super user accounts shall be reviewed on a quarterly basis and passwords changed as per "Quarterly Review of Admin, Super user and Generic accounts"

15.ENCRYPTION

All laptops and desktops shall make use of full drive encryption where possible. All removable drives should be encrypted before company data is stored. When transmitting sensitive data, encryption shall be used.