SAMUEL HODGE GROUP SECURITY POLICY

Policy title:	**Samuel Hodge Group of Companies, Including , Samuel Hodge, Victor Marine, RLBS and Teknequip Information Security Policy**

Issue date:	20/07/2023	**Date policy is to be reviewed:**	***20/07/2023***

Version:	1.1	**Issued by:**	David jones

Scope:	

Associated documentation:	Group Password Policy New Hardware Setup Procedure
Appendices:	
Approved by:	Neal Crisford (Managing Director)
Date:	20/07/2023

Review and consultation process:	Annual Review at QMS Meeting
Responsibility for Implementation & Training:	Day to day responsibility DAVID JONES (Group IT Manager) Day to day responsibility for training: DAVID JONES

Revisions:

Date:	**Author:**	**Description:**
01/07/2023	David Jones	Version 1.0 First Copy

Distribution	Policy is to be distributed via email attachment in PDF form. Also available from the IT department on request.

Contents

1. Introduction

This information security policy is a key component of The Samuel Hodge Group of Companies, Including, Samuel Hodge, Victor Marine, RLBS and Teknequip's management framework. It sets the requirements and responsibilities for maintaining the security of information within The Samuel Hodge Group of Companies, Including, Samuel Hodge, Victor Marine, RLBS and Teknequip. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

2. Aim and Scope of this policy

- The aims of this policy are to set out the rules governing the secure management of our information assets by:

  - preserving the **confidentiality, integrity and availability** of our business information
  - ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies
  - ensuring an approach to security in which all members of staff fully understand their own **responsibilities**
  - creating and maintaining within the organisation a level of **awareness** of the need for information
  - detailing how to **protect** the information assets under our control

- This policy applies to all information/data, information systems, networks, applications, locations and staff of The Samuel Hodge Group of Companies, Including, Samuel Hodge, Victor Marine, RLBS and Teknequip or supplied under contract to it.

3. Responsibilities

- Ultimate responsibility for information security rests with the Chief Executive of The Samuel Hodge Group of Companies, Including, Samuel Hodge, Victor Marine, RLBS and Teknequip, but on a day-to-day basis the Group IT Manager and Assistant Group IT Manager shall be responsible for managing and implementing the policy and related procedures.
- Responsibility for maintaining this Policy, the business Information Risk Register and for recommending appropriate risk management measures is held by the Group IT Manager. Both the

Policy and the Risk Register shall be reviewed by the Group IT Manager at least annually.

- Department Managers are responsible for ensuring that their permanent staff, temporary staff and contractors are aware of:-
    - The information security policies applicable in their work areas
    - Their personal responsibilities for information security
    - How to access advice on information security matters

- All staff shall comply with the information security policy and must understand their responsibilities to protect the company's data. Failure to do so may result in disciplinary action.
- Department managers shall be individually responsible for the security of information within their business area.
- Each member of staff shall be responsible for the operational security of the information systems they use.
- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4. Legislation

- The Samuel Hodge Group of Companies, Including, Samuel Hodge, Victor Marine, RLBS and Teknequip] is required abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations.
- The requirement to comply with legislation shall be devolved to employees and agents of the Samuel Hodge Group of Companies, Including, Samuel Hodge, Victor Marine, RLBS and Teknequip, who may be held personally accountable for any breaches of information security for which they are responsible.
- In particular, the Samuel Hodge Group of Companies, Including , Samuel Hodge, Victor Marine, RLBS and Teknequip is required to comply with:
    - The Data Protection Act (1998)
    - The Data Protection (Processing of Sensitive Personal Data) Order 2000.
    - The Copyright, Designs and Patents Act (1988)
    - The Computer Misuse Act (1990)
    - The Health and Safety at Work Act (1974)

- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

5. Personnel Security

Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
- References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity.
- Information security expectations of staff shall be included within appropriate job definitions.
- Whenever a staff member leaves the company their accounts will be disabled the same day they leave.

Information Security Awareness and Training

- The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.
- Information security awareness training shall be included in the staff induction process and shall be carried out annually for all staff
- An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information security is maintained and updated as necessary.

Intellectual Property Rights

- The organisation shall ensure that all software is properly licensed and approved by the Group IT Manager and Assistant Group IT Manager. The Samuel Hodge Group of Companies, Including, Samuel Hodge, Victor Marine, RLBS and Teknequip and individual intellectual property rights shall be protected at all times.
- Users breaching this requirement may be subject to disciplinary action.

6. Access Management

Physical Access

- Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data. A log of these personnel are kept and reviewed annually.

Identity and passwords

- Passwords will comply with the Group Password Policy, included with the associated documentation.

User Access

- Access to information shall be based on the principle of "least privilege" and restricted to authorised users who have a business need to access the information.

Administrator-level access

- Administrator-level access shall only be provided to individuals with a business need who have been authorised by the Group IT Manager.
- A list of individuals with administrator-level access shall be held by the Group IT Manager and shall be reviewed every 12 months
- Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.

Application Access

- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.
- Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

- Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only

System Perimeter access (firewalls)

- The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.
- All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.
- The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly

- All firewalls shall be configured to block all incoming connections.
- If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.

Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.
- The business reserves the right to monitor and systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

7. Asset Management

Asset Ownership

- Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

New Asset Procedure

- Any new hardware being added to the company must first be proposed and then approved by either the Group IT Manager or the Assistant Group IT Manager.
- Upon purchase new hardware assets will be assigned a serial number and owner and be added to the Physical asset register. They will then be setup in accordance with the “New Hardware Setup Procedure”.

Asset Records and Management

- An accurate record of business information assets, including source, ownership, modification and disposal shall be maintained.
- All data shall be securely wiped from all hardware before disposal.
- physical assets defined by Victor marine with V on asset register, RLBS with R, Samuel Hodge with S and Teknequip with T

Asset Handling

- The Samuel Hodge Group of Companies, Including, Samuel Hodge, Victor Marine, RLBS and Teknequip shall identify particularly valuable or sensitive information assets through the use of data classification.
- All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.
- All company information shall be categorised into one of the three categories in the table below based on the description and examples provided:

Category	**Description**	**Example**
Public	Information which is not confidential and can be made available publicly through any channels.	• Details of products and services on the website • Published company information • Social media updates • Press releases
Amber Information	Information which, if lost or or made available to unauthorised persons could impact the company's effectiveness, benefit competitors or cause embarrassment to the organisation and/or its partners	• Company operating procedures and policy • Client contact details • Company plans and financial information • Basic employee information including personal data

Red Information	Information which, if lost or made available to unauthorised persons, could cause severe impact on the company's ability to operate or cause significant reputational damage and distress to the organisation and/or its partners. This information requires the highest levels of protection of confidentiality, integrity and availability.	• Client intellectual property • Data in e-commerce systems • Employee salary details • Any information defined as "sensitive personal data" under the Data Protection Act

Removable media

- Only company provided removable media (such as USB memory sticks and recordable CDs/DVDs) shall be used to store business data and its use shall be recorded in the removable media register. (e.g. serial number, date, issued to, returned).
- Users must fill out a Request for Removable media Device form which states the size of device required and length of time required. All forms are to be reviewed by the Group IT Manager before devices are released into the users care.
- Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of the Group IT Manager before they may be used on business systems. Such media must be scanned by anti-virus before being used.
- Where indicated by the risk assessment, systems shall be prevented from using removable media.

Users breaching these requirements may be subject to disciplinary action.

Mobile working

- Where necessary, staff may use company-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements
- Use of mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the Group IT Manager.
- Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.

- Users must inform the Group IT Manager and Assistant Group IT Manager immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

Personal devices / Bring Your Own Device (BYOD)

- Where necessary, staff may use personal mobile phones to access business email. This usage must be authorised by the Group IT Manager . The device must be registered in the asset records and must be configured to comply with the mobile working section and other relevant sections of this policy.
- No other personal devices are to be used to access business information

Internet Usage

- Users are permitted to use the internet subject to the Samuel Hodge Internet Usage Policy

Social Media

- Users are permitted to use social media subject to the Samuel Hodge Social Media Policy

End of Life

- Devices which are considered "End of Life" will be brought to the IT department where the asset register will be updated to show that the device is no longer in circulation.
- For Mobiles and Tablets, all functioning devices will be wiped before being placed in WEE waste.
- For Laptops and Desktops, all hard drives will be removed from the devices, the platters removed from the cases and sandblasted within the facilities to ensure all data cannot be recovered.
- The rest of the computer will be placed in WEE waste

8. Software Management

New Software Procedure

- Any new software that's to be added to The Samuel Hodge Group of Companies, Including , Samuel Hodge, Victor Marine, RLBS and Teknequip must first be submitted to the Group IT Manager, using the New Software Submission form.

- Once the form is submitted either the Group IT Manager or Assistant Group IT Manager will perform a Risk Based Analysis on the software and determine if the software is suitable for the business environment, as well as checking recommended specification and if there would be any additional hardware requirements.

- If the software is approved it needs to be documented in the Approved Software Register.

9. Physical and Environmental Management

- In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security accreditation should be applied if necessary.
- Systems shall be protected from power loss by UPS if indicated by the risk assessment.
- Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.
-

10. Computer and Network Management

Operations Management

- Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Group IT Manager.

System Change Control

- Changes to information systems, applications or networks shall be reviewed and approved by the Group IT Manager.

Accreditation

- The organisation shall ensure that all new and modified information systems, applications and networks include security provisions.
- They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by the Group IT Manager before they commence operation.

Software Management

- All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.

- All software security updates/patches shall be installed within 7 days of their release.
- Only software which has a valid business reason for its use shall be installed on devices used for business purposes
- Users shall not install software or other active code on the devices containing business information without permission from the Group IT Manager.
- For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes.

Local Data Storage

- Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least monthly).
- A backup copy shall be held in a different physical location to the business premises
- Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

External Cloud Services

- Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.
- Currently approved external cloud services include:
  - Windchill document control
  - Visual Manufacturing ERP
  - Office 365 – Sharepoint OneDrive and other Office 365 products

Protection from Malicious Software

- The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
- All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system
- All anti-malware software shall be set to:
  - scan files and data on the device on a daily basis
  - scan files on-access

    - automatically check for, and install, virus definitions and updates to the software itself on a daily basis
    - block access to malicious websites

Vulnerability scanning

- The business shall have a yearly vulnerability scan of all external IP addresses carried out by a suitable external company
- The business shall act on the recommendations of the external company following the vulnerability scan in order to reduce the security risk presented by any significant vulnerabilities
- The results of the scan and any changes made shall be reflected in the company risk assessment and security policy as appropriate.

11. Response

Information security incidents

- All breaches of this policy and all other information security incidents shall be reported to the Group IT Manager.
- If required as a result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the Group IT Manager
- Information security incidents shall be recorded in the Security Incident Log and investigated by the Group IT Manager to establish their cause and impact with a view to avoiding similar events. The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.

Business Continuity and Disaster Recovery Plans

- The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Reporting

- The Information Security Officer shall keep the business informed of the information security status of the organisation by means of regular reports to senior management.

Further Information

- Further information and guidance on this policy can be obtained from David Jones (Group IT Manager), email David.jones@samuelhodge.co.uk or call 07793587919. Comments and suggestions to improve security are always welcome.

Policy approved by:

Signature____
Date_ 01/07/23

[Neal Crisford CEO of the Samuel Hodge Group of Companies, Including, Samuel Hodge, Victor Marine, RLBS and Teknequip]