Information Security Policy

Document Control:

Document filename	Information Security Policy		
Director Lead	Jon Russell	**Status**	Live
Owner	Jon Russell	**Version**	V08
Author	Christopher Pratt	**Version Date**	June 2026
Retention period	Review Annually	**Configuration control**	No
Confidentiality	Private	**Distribution**	Moorhouse Consulting/Customer

16th Floor, Dashwood House, 69 Old Broad St, London EC2M 1QS
+44 (0)20 3004 4482

Version Control:

Version	Date	Notes	Completed by
V01	20/03/2017	Document creation and draft	Christopher Pratt
V02	01/02/2019	Revision	Jon Russell
V03	03/08/2020	Revision	Jon Russell
V04	12/10/2021	Revision following extended home working by workforce caused by Covid pandemic	Christopher Pratt
V05	27/04/2022	Objectives section updated	Christopher Pratt
V06	01/03/2023	New Expleo template, minor edits to reflect lessons learn	Christopher Pratt
V07	13 January 2025	Add Umbrella and Qualys information	Christopher Pratt
V08	June 2026	Annual review no update	Ethan Box

MOORHOUSE
AN EXPLEO COMPANY

Table of Contents

1. Why do we have an Information Security policy?

Moorhouse are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the firm in order to:

- Preserve our quality of service to clients;
- Comply better with legal, regulatory and contractual requirements;
- Ensure we retain a competitive edge;
- Safeguard our commercial reputation;
- Protect our profitability.

We will achieve this by developing and implementing a combination of people, process and technology controls to mitigate information security risks according to Moorhouse's defined level of risk and the desired objectives (including maintaining the ability to share knowledge) – balancing usability and security.

This Information Security policy is part of the Moorhouse Information Risk Management framework to manage the risks to its technology, systems and information assets and as such is central to the overall cyber security strategy of Moorhouse. Our risk management framework allows the systematic identification, assessment and response to information-related risks.

The Information Security Policy and associated documents are reviewed continually and updated at least annually to ensure continued alignment with our business environment.

This policy applies to:

- All employees and associates of Moorhouse and third-party suppliers.
- Technologies or services used to process Moorhouse information assets.
- Information that is processed on behalf of Moorhouse.
- Information that Moorhouse is processing on behalf of another party.

Moorhouse has a series of policies to address specific areas of Information Security due to the depth and breadth of coverage required. This policy should be read in conjunction with:

• Information Security Manual	• Incident Management Policy
• Acceptable Use of Assets Policy	• IT Security (Access) Policy
• Client Site Policy	• Risk Management Policy
• Continuity Management Plan	• Cryptographic Controls
• Physical Security and Clear Working Environment Policy	• IT Access Controls

2. Objectives

This Policy is designed to:

- Protect the information assets and technology by identifying, managing and mitigating information security threats and risks. This will be achieved through a monthly threats, risk and issues meeting where we will discuss and log updates to, and maintenance of, risk treatment plans.

- Define security controls that are effective, sustainable and measurable. This will be achieved through the production of management dashboard that are reviewed by Leadership team each month.
- Assist in the compliance of contractual, legal or regulatory obligations. This will be achieved through annual review sessions with subject matter experts.
- Identify, contain, remediate and investigate information security incidents to maintain and assist in improving information security. Incidents are reported in our management Dashboard. This will be achieved through formal review of all incidents raised and needed improvements added to continuous improvement plan.
- Ensure that Moorhouse is compliant with its information security obligations. This will be achieved through annual internal and external reviews and testing and resultant reports shared with leadership.
- Provide assurance to other parties that Moorhouse has a robust control environment in place to protect their data through an effective information security management system. This will be achieved through internal and external audits of client projects which will be done annually and led by the IMS audit review team leader.
- Annual training and development for all existing staff. and clear defined on boarding programme to integrate new starters into Moorhouse. New starter training must be completed within the first month of starting and reviewed with their Line Manager. Annual training must be tracked and reviewed to ensure timely completion. Ad hoc training be developed to counter market trends and support business security posture. All training will be e-learning based to ensure it is accessible and available to staff as required. This will be achieved through P&T monitoring and review of on-boarding and annual training of all staff. The P&T advisors will review their teams development and feed into each individual POS.
- The Continuous Improvement process will provide the control that our policies, processes and procedures are evergreened and reflect business goals. This will be achieved through maintenance of Continuous Improvement plan, annual review of policy and procedures and a separate annual review by Knowledge Management team to ensure currency and accuracy of published documentation
- Our IT Supplier chain must support our business strategy and help drive change. Suppliers align to our code of conduct. There will be a quarterly performance review, with (a) Microsoft platform (b) SalesForce platform (c) data waste management .

3. Responsibilities for Information Security

The Partner team has overall executive responsibility for Information Security. They must actively support the adoption and implementation of the information security requirements and Policy.

Day to day responsibility for ensuring that client information is protected is the responsibility of the relevant Partner lead for each client.

The Finance and Operations Director is accountable for ensuring adequate and effective information security controls are in place across the organization.

This Policy is owned, managed and developed by the Information Security Manager, acting for the Operations and Finance Director on behalf of Moorhouse

The Board will regularly review risks to technology and systems.

The Moorhouse Consulting Executive Committee (ExCo) meets on a monthly basis to discuss matters relating to the strategy of the firm including information security. ExCo represents the steering group to support the commitment to information security management. ExCo includes as members executives and specialists as required to support the ISMS and periodically to review the security policy.

All individuals within scope of the Policy must comply with the Policy and ensure that reasonable effort is made to protect the information and technology assets of Moorhouse from accidental or unauthorised disclosure, modification or destruction.

Moorhouse will expect both employees and their contractors (known as Associates) to support the information security posture.

Employees will have user profile and training to help them met and maintain the information security posture.

Associates will also have a user profile and training but in most instances will provide their own hardward and software. Access to network and monitoring will be performed to ensure they respect and adhere to our policies and procedures.

Resources will be monitored to identify user behaviors which may cause risks or violations to our policies and procedures. The employee contract will provide disciplinary process.

Role	Mapped to Moorhouse position	Key Tasks
Information Security Director	Finance and Operations Director	Owner of Policy Accountable for IT Services
Information Security Manager	Compliance Manager	Responsible for day to day ITC management
Information Security Management System Manager	Compliance Manager	Responsible for maintenance of ISMS documentation and ever-greening. Responsible for co-ordination of ISO 27001 audits and evidence collection

4. Guiding Principles

The risks and mitigating activities to protect information assets should be aligned with our business goals. Security controls must be proportionate to the defined classification.

These were determined while completing a Statement of Applicability and the resultant Information Security Management System (ISMS) is designed to balance the need to share information with the need to reduce information-related risks to acceptable levels. The ISMS is used to ensure that the objectives of this Information Security Policy are satisfied.

The ISMS ensures that business continuity plans, data backup procedures, protection from viruses and hackers, access control to systems and information security incident reporting are fully supportive of this Information Security Policy. Control objectives for each of these areas are contained in Moorhouse's Information Security Manual, which is the core of our ISMS, and further support is derived from specific, documented policies and procedures.

Where Moorhouse clients require services to be provided using the Client's Information Systems, individuals delivering these services, whether Employed, Associate or Third Party, must use these systems according to the Client's Policies and Procedures.

An information security risk assessment must be carried out wherever a third party provider is used for any services which involve contact with Moorhouse information.

5. Approach

Moorhouse will consider the application of recognised sources of security management good practice. In particular, Moorhouse aims to meet the standards of ISO27001.

Moorhouse will make use of endorsed assurance schemes. Moorhouse will maintain certification for Cyber Essentials to demonstrate commitment to cyber security.

Moorhouse will facilitate a 'security aware' culture and promote that Information Security is everyone's responsibility.

Moorhouse will educate users and maintain awareness and promote good behaviours with appropriate training relevant to the role and regular refreshes.

Engagement Managers shall understand and assess the cyber security risks of each Project including recognising the sensitivity of information and good cyber behaviours.

Back-up and disaster recovery plans, processes and technology, are in place to mitigate risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services.

6. Audits and Continuous Improvements

Moorhouse will undertake annual internal audits to review progress of the organisation and allow regular staff engagements to ensure adoption and opportunities to improve.
A schedule will be maintained to show planned audits and improvements for the following two years.
These audits, reports and findings will be shared with Exco for decisions.
The Quality team will lead the audits in consultation with the Information Security Manager and Operations Director.

7. Policy Enforcement

Any breach of this policy will be treated seriously and could result in disciplinary action being taken against an employee in accordance with the company's disciplinary policies. In the event of a criminal offence being committed this could result in criminal proceedings against the employee.

If a user suspects or discovers any material breach of the requirements detailed within this Policy, they must report this in line with the Incident Management Policy.

Glossary

Term	Definition
Confidentiality	Information is not made available or disclosed to unauthorised individuals, entities or processes.
Integrity	Information's accuracy, validity and completeness is protected.
Availability	Information is accessible and usable upon demand by an authorised entity
Threat	A threat is anything that is capable, by its action or inaction, of causing harm, either directly or indirectly, to a Moorhouse information asset. A threat exploits a vulnerability to cause impact to a Moorhouse information asset.
Control	Means of protecting the confidentiality, integrity and/or availability of Moorhouse information, including policies, standards, procedures, processes or practices, which can be of administrative, technical, management or legal nature. Controls can be detective, preventative or reactive.
Information asset	A body of information that can be understood, developed or shared and has value to Moorhouse.
External	Anything which is not owned, managed, employed or provided by Moorhouse.
Internal	Anything which is owned, managed, employed or provided by Moorhouse.
Information security management	A systematic approach to managing information within a predefined acceptable range so that it remains secure. It includes people, processes and technology by applying a risk management process.
Risk	The chance or possibility of uncertainty on objectives, expressed as a combination the probability of an event occurring and the impact such an event would have on the achievement of one or more objectives.
Contractual obligation	Requirements set when entering a contract with another party.
Legal obligation	Legal requirements, e.g. Data Protection Act 1998 or General Data Protection Regulation (GDPR), Computer Misuse Act 1990.
Regulatory obligation	Requirements set out by a Regulator, e.g. UK ICO, NHS, etc.
Information Security Incident	An event or series of events that compromises the confidentiality, integrity or availability of Moorhouse information.
Risk assessment	Structured process for examining information security threats, vulnerabilities and impacts relating to a given system or situation to determine whether an individual control is required or operating as expected.

Risk management	The process of identifying and managing information security risks. Once identified risk are treated by mitigating them, accepting them, transferring them or stopping the process with which they are associated.