Information Security Policy

Information security is an integral part of Wood's management and business processes. Wood is committed to ensuring that all information and assets it manages are protected from activities that could compromise the confidentiality, integrity and availability of the resource. One of the most important ways this is achieved is by reminding everyone that Information Security is a shared responsibility. Everyone in Wood has a role to play in helping to protect our shared resources and data.

Purpose:

The purpose of this policy is to outline an effective information security and risk management framework that combines administrative, physical, and technical controls to protect the confidentiality, integrity, and availability of Wood information and assets. It provides the baseline for a robust security culture, setting rules for expected behaviours and defining steps required to monitor, investigate, and minimize information security risk to Wood.

Scope:

This policy applies to all workers and includes employees and contingent workers, non-Wood workers including contractors, joint ventures, third parties, or other agents (hereafter referred to as "user") engaged by Wood worldwide. Where these standards are not followed, this should be highlighted to the Vice President, IT Infrastructure and Cyber Security.

Policy Requirements:

The following sections define the specific requirements for various roles within the organization.

Management Commitment to Information Security

The Executive Leadership Team (ELT) have direct accountability for the security of information assets within the organization through clear direction, demonstrated commitment, explicit assignment, adequate resourcing and acknowledgment of information security responsibilities.

Wood Line Managers

- Wood line managers must understand what information and information assets support their business, including any information being processed or held on behalf of Wood by third parties.
- Wood line managers must ensure that access to information and information assets is authorised, appropriately restricted, and immediately removed from individuals who change role or terminate employment with Wood.
- Wood line managers must determine the necessary competence of their team's roles with responsibilities that affects information security performance. They must ensure that persons assigned to these roles are competent on the basis of appropriate education, training, or experience. Where applicable, they must take actions to acquire the necessary competence and evaluate the effectiveness of the actions taken and retain appropriate documented information as evidence of competence.
- Wood line managers are responsible for reading and understanding all internal security policies and are accountable for ensuring all direct reports are aware of and compliant to the same policies, follow documented processes as well as relevant regulatory requirements and applicable legislation.
- Wood line managers must ensure that any additional risk management processes required by legal, regulatory, or contractual commitments applicable to operational geography are applied.
- Wood line managers must ensure that all direct reports abide by the IT Acceptable Use policy and have completed any assigned mandatory cyber security training.
- Wood line managers must ensure that movers and leavers are submitted into the appropriate People and Organisation process.
- Wood line managers must report non-compliance of this policy to the IT Risk and Compliance (RC) team at isrm@woodplc.com.

Wood IT Function

- The Chief Information Officer (CIO) must ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated, with responsibilities and behaviours relating to information security clearly defined, communicated, and understood by all teams inside Wood IT.

- The CIO must appoint leadership for the information security function.
- The Vice President, IT Infrastructure & Cyber Security must
  - define, document, and communicate a clear and appropriate security organisational structure with the organisation and to other interested parties.
  - assign responsibilities and authorities for reporting performance of the information security management system within the organisation.
  - report to Wood Head of Internal Audit and Risk on key information security risks and the effectiveness of implemented controls and contingencies.
  - report any exceptions to this policy to the CIO.
- The information security team must:
  - establish and maintain appropriate contacts with special interest groups or specialist security forums.
  - lead investigations where Wood is at risk of an internal or external information security breach.
- IT Risk and Compliance must maintain a control register to document all security controls required to protect information assets, maintain compliance to contractual, legislative, regulatory and relevant industry standards required by Wood and its clients.
- Wood IT must support investigations where Wood is at risk of an internal or external information security breach.
- Wood IT must ensure segregation of duties are implemented in line with the appropriate policy, procedure, or work instruction.
- Wood IT must undertake a security-by-design approach to ensure information security is a crucial consideration regardless of the type of project.
- Wood IT is responsible for implementation, maintenance, and continual improvement of an Information Security Management System (ISMS) based on applicable industrial standards such as ISO/IEC27001, SOC2 or NIST.
- Wood IT is responsible for annual review and maintenance of the information security objectives in partnership with the business and wider IT strategy.

Wood Users

- Wood users must immediately report any suspected information security incidents and violations including, but not limited to, theft or loss of Wood information or a Wood IT asset containing Wood information, to the IT Service Desk and their line manager.
- Wood users must understand the information security risks within the use of information assets, including the causes and consequences associated with them. When in doubt, Wood users must consult the RC team, who can advise on security risk management processes, including those related to third parties with whom Wood may work.
- Wood users must read and abide by the information security requirements set out in the IT Acceptable Use Policy and other information security policies.
- Wood users must complete all assigned information security training and education to manage specific security risks relevant to their location and/or business.

Definitions:

Information Assets - Any Wood or customer information that is essential to an organisation's business and therefore needs to be protected appropriately. Information assets includes hardware (including desktop, laptop, tablet computers and mobile devices), software (both purchased and licensed but also freeware), information (not limited to electronic media such as databases, websites, electronic files but also paper and other forms including unrepresented information in the form of knowledge of the employees).

Reference Documents:

- IT Acceptable Use Policy, GIT-POL-110007
- IT Risk Management Policy, GIT-POL-110004

Name	Ron Beckman
Position	Chief Information Officer
Date	01 November 2024