IT Acceptable Use Policy

Purpose:

This Wood IT Acceptable Use Policy (AUP) defines rules and guidance on appropriate and safe use of Wood information assets.

Scope:

This policy applies to all company information assets and all remote, agile, mobile, office-based workers and includes employees and contingent workers, non-workers including contractors, joint ventures, third-parties, or other agents (hereafter referred to as "users") who have or are responsible for an account or on any devices with access to the network or Wood non-public information. All exemptions required by individuals where not prohibited by law must be approved by the Vice President IT Infrastructure & Cyber Security.

Breaches of this policy could result in disciplinary action in accordance with Wood People & Organisational processes and legislative requirements. Localised regulations will supersede statements within this policy, and it is the users' responsibility to confirm if more stringent requirements apply to where they are currently working.

Policy Requirements:

General Use and Ownership

1. New users must read and acknowledge this IT AUP as part of their onboarding process.
2. All existing users are required to take mandatory cyber security awareness training, including reading, and formally acknowledging the IT AUP on an annual basis.
3. Users who have access and use information assets are required to protect them against loss, damage, theft, and possible misuse by others and in accordance with this policy.
4. Users must only access information assets provided to them for duties in conjunction with their employment, information asset classification, and in accordance with their terms and conditions of employment or equivalent. Unauthorised access to information assets is prohibited.
5. Administration rights for information assets are granted only by exception and in conformance with the Administrative Rights Policy.
6. Users must return all Wood information assets on termination of employment or contract including but is not limited to laptop, desktop, memory sticks and mobile phones or any devices that provides access to Wood information and systems.
7. Wood has the right to audit and monitor all activities and information related to information assets, subject to applicable laws and jurisdiction, and reserves the right to ensure appropriate business conduct.

Unacceptable Use

8. Information assets must not be used for the access, creation, display, storage, transmission, or deliberate reception of any offensive material.
9. There is a legal requirement for the Company to report any computer crime involving child pornography to the police. A user who receives an email connected with child pornography, must report this to the IT Service Desk immediately.
10. Infringement of copyright by copying or transmitting copyright material without permission of the copyright holder ("fair use" notwithstanding) is forbidden.
11. Use of information assets for any public or private broadcast of television programmes or films, electronic games or other entertainment media is forbidden.
12. Users must not use Wood's information assets for non-company commercial activities such advertising, running personal business or fundraising for commercial or charitable organizations not directly connected with Wood.
13. Deliberate activities which could lead to any of the following consequences are prohibited:
    - Corrupting or destroying information assets
    - Misuse of information assets (e.g. in a way that denies service to others, overloads the network).

Information Security

14. Users must create and protect passwords in adherence to the Password Policy and the Password Construction Standard.
15. Attempting to remove or bypass any security access on any Wood information assets is forbidden.
16. Users must not install any software on Wood devices without approval from Wood IT.
17. All software must be approved, purchased, installed, and configured in accordance with the IT Software Policy.
18. Users must comply with the Clean Desk Clear Screen Policy and not leave any information asset unattended without either logging out or activating a password-protected screensaver.

19. Users must ensure that any printouts are protected and disposed of appropriately.
20. Users must immediately report to the IT Service Desk, any known or suspected breaches of information security.
21. Possible breaches include theft or loss of information assets; unauthorised disclosure of proprietary or sensitive or secret information, system, or device access; and disclosure of Wood or client information. If a breach of security is recorded, the burden of proof will be on the registered user to show that they are not responsible for the breach.
22. Users must not use Wood information assets to store any non-work information.
23. All information to be stored in accordance with Wood Data Protection Policy and Data Storage Guideline.
24. Wood information may be used, but not stored permanently, on non-Wood information assets subject to these guidelines, except where disallowed by local-specific or business-specific requirements:
    - Where Wood information asset devices or systems do not meet the needs of a user or project and additional controls are required, requests should be submitted through the IT Service Desk
    - When using a non-Wood information asset device users must ensure that anti-virus software and a firewall have been installed and are regularly updated.
25. Only Wood IT approved, or client mandated, file sharing services must be used to exchange company information. Use of other public file sharing or cloud-based services is prohibited.
26. Users must never send non-public information, enter passwords, or provide account information over an insecure connection.
27. All information must be processed fairly and for legitimate purposes only, ensuring the destination of the data is secure and in conjunction with the Data Protection Policy.
28. No personal devices (including USB drives) are to be connected to the Wood IT environment.
29. The use and handling of removable media storage must be in accordance with the Removable Media policy.

Equipment

30. To ensure a consistent, secure, supportable, and efficient environment employees will be provided with a single set of IT equipment upon hire.
    - This includes one computer, one keyboard, one mouse, one docking station (if applicable), and up to two monitors.
    - Requests for additional equipment will be granted only when required.
31. Employees who work at multiple locations will be provided with a laptop which will travel with employees as needed.
32. Peripherals such as monitors, keyboards, and docking stations are expected to remain at the employee's primary work location.

Internet and Email

33. Where Wood provides users with access to the internet, it is primarily provided for work-related purposes. Reasonable personal use is permitted, subject to these restrictions:
    - Managers can limit or deny users' personal access to the internet
    - Users' personal use of the internet must not interfere with the performance of duties or adversely affect system performance
    - Wood will not accept liability for personal legal action resulting from any user's misuse of the internet
34. Wood IT will restrict internet access to prevent abuse of network resources or infringement of copyright.
35. Wood reserves the right, consistent with local law, to monitor internet access, including but not limited to email and web access.
36. Users must not publish other colleague's personal information on the internet without the express consent of every individual concerned.
37. Users must act in accordance with the Cloud Services Policy and must not upload other users, Wood, client, or personal information to unauthorised cloud services.
38. Users must not use personal email for Wood business purposes, or Wood email address for personal use.
39. When communicating electronically, users must conduct themselves in an honest, courteous, and professional manner.

40. The size of users' emails (both sent and received), the frequency of transmission and the number of recipients must not be excessive and may be monitored to ensure system performance.
41. Users must not send or forward email to a distribution list or large groups of users unless there is a genuine requirement.
42. Users must treat attachments and hyperlinks received via email/electronically e.g. via Teams with caution and consider whether the email is expected, is it suspicious, could it have been spoofed, and when in doubt the user must check with the originator via a known and trusted contact method.
43. Users must report suspicious emails using the Phish Alarm button in Outlook (or menu via mobile application) or forward to phishing@woodplc.com.
44. Forging an email (or any other electronic message) or sending email from any account other than one's own without permission may be treated as fraud.
45. Users sending emails from any Wood account or Wood owned domain name for the purpose of promoting, advertising, marketing, or selling of a product or service or promoting Wood's brand(s), must do so in accordance with anti-spam laws.
46. Email must not be used for primary information storage.

Social Media and Messaging

47. In line with the Social Media Policy, users must not use social media in a way that could potentially breach the Wood Code of Conduct or compliance with Wood policies. Social Media messaging applications and other non-Wood tools or applications must not be used to transmit any confidential, sensitive or secret information.

Third-Party Information Assets

48. Third-party devices must not be connected to the Wood corporate network but may use the guest wireless.
49. The use of third-party information assets is permitted if the business circumstances are justified. Users must exercise the same level of care in the use of these information assets as is expected by Wood or in accordance with third-party guidelines.
50. Third-party products and services such as hardware, software, cloud platform, infrastructure as a service must be assessed in accordance with the IT Risk Assessment Procedure - Third-Party and will not be integrated into the Wood environment without Wood IT approval.
51. Wood IT devices must not be connected to third-party networks other than to use the Internet for VPN access.

Remote Users

52. Wood will determine, with information provided by the user, the line manager/project manager and in accordance with this policy, the appropriate IT equipment required (including hardware, software, mobile device, etc.) for successful execution of the remote user job responsibilities.
53. Remote users must protect unauthorized access to Wood information assets from other persons using the same premises. Whenever possible, remote working must be done in a separate room or workspace that can be locked or secured from the rest of the house or co-working space.

Artificial Intelligence

54. For acceptable, secure, and ethical use of Artificial Intelligence (AI) within Wood users must comply with the Wood Artificial Intelligence Policy.

Definitions:

Confidential Information - Means (i) all information of a confidential nature concerning the trade secrets or business dealings, pricing, plans, procedures, products, services or strategies of Wood, its Affiliates and third parties to whom Wood owes a duty of confidence; (ii) any document or information asset designated as confidential; and (iii) any information which by its nature the recipient ought reasonably to conclude is confidential information, in all cases whether encrypted or not and including all copies of the above on any media.

Information Assets - Any Wood or customer information that is essential to the business and needs to be protected appropriately. Information assets include 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 users).

Mobile/Agile/Hybrid user - User who works at various locations on a frequent basis (home and/or multiple offices and/or client sites and/or hot-desk) and requires standard applications and/or light touch/view Engineering applications which might include some CAD users.

Offensive Material - Material that includes but is not limited to religious or political convictions or opinions; and text or images that are abusive, sexist, racist, pornographic, harassing, discriminatory, derogatory, obscene, or defamatory.

Office based user - User who performs tasks full-time from a Wood Office or Design & Engineering tasks from the office with only very occasional need for remote access/working.

Personal Information - Also often referred to as "personal data" and which also captures data that can be referred to as Personally Identifiable Information (PII) - any information relating to an identified or identifiable natural (living) person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, location date, online identifiers or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity.

- Examples of Personal Information in the employment context include but are not limited to: identification data (such as name, address, date and place of birth, photograph); contact details (such as telephone number, email, address); national identifiers (such as ID numbers, tax IDs/social security numbers, driver's licence number, passport number); education and training (educational history, professional qualification and experience, professional organisations, publications); and professional status (such as title, position, location).
- Examples of this Personal Information in a client or candidate context includes name and contact details on our CRM databases, email addresses, IP address, newsletter subscriptions and marketing preferences.
- Examples of sensitive Personal Information include but are not limited to information relating to a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for identifying a person), health data, data about sex life or sexual orientation and information relating to criminal convictions and offences or related security measures.

Proprietary Information - Information or intellectual property owned by the client or third-party that must be processed by Wood.

Remote user - User primarily based at one remote location (e.g., home), works in a Wood office or off-site location infrequently and requires only standard business applications.

Reference Documents (BMS):

- Artificial Intelligence Policy, GIT-PLD-110007
- Social Media Policy, CMN-PLD-110002
- IT Risk Management Procedure, GIT-PRO-110002
- Cloud Services Policy, GIT-POL-110018
- Data Protection Policy, COP-PLD-100007
- Data Storage Guideline, KB0011773
- Removable Media Policy, GIT-POL-110010
- Intellectual Property Assets Policy, LGL-POL-110002

Ronald Beckman

Name	Ron Beckman
Position	Chief Information Officer
Date	24 January 2025