INFORMATION SECURITY POLICY

This policy sets out the rules and procedures that directors, employees, workers, consultants and interns of Sahita Human Capital Solutions Pvt Ltd ("**Sahita**") are required to follow while accessing information ("**Sahita Information**") using information systems including hardware, services, facilities, and processes owned, made available, or which are connected to Sahita's managed networks and servers including any personally owned devices that are used in connection with Sahita's business.
Sahita has the right to extend the applicability of this policy to classes of individuals or organizations who may otherwise access, handle, or process information on our behalf or in relation to their engagement with Sahita.

"Cybersecurity incident" means any type of cybersecurity incidents as mentioned in Appendix – A of this policy.

Information governed by this policy

Sahita is the exclusive owner of all information and data that is created, received, or maintained as part of its business operations (subject to third party rights). Sahita's information does not belong to any director, employee, worker, consultant or intern of Sahita.

Sahita's personnel will be given access to information as needed for their assigned functions in the company on a "need-to-know" basis. If the function changes, access to information may be reviewed accordingly and information that the concerned individual could previously access may be restricted.
To the extent possible, Sahita Information shall be classified as per Appendix – B of this policy.

Unless otherwise marked, Sahita personnel must treat all information as Confidential Information regardless of its source or form and must not make it available for public disclosure without prior authorisation.

It shall be the responsibility of every Sahita personnel to ensure confidentiality of Sahita Information and to use best efforts to safeguard Sahita Information from theft, loss, misuse, damage, destruction and unauthorised access.

Sahita personnel shall not use any unauthorised devices or programs to access or use Sahita Information. Personal mobile devices and systems may be used, subject to controls established by Sahita that may change from time to time, to access public information and Confidential Information shared over email communications.

Sahita Information that are classified as Highly Confidential Information should be shared within the organisation only using secure file sharing methods and must be password protected. Passwords should be shared separately. Personal devices and systems should not be used to access, share or transmit Highly Confidential Information.

Sahita personnel shall not remove any data or document from storage drives (physical or cloud) made available by Sahita, or transfer onto any portable device any Confidential Information or Highly Confidential Information unless it has been approved by the IT Department for such removal or transfer.

IT assets governed by this policy

IT assets (listed below) made available to you may be taken back at the discretion of Sahita.
(i) Desktops, laptops and tablets provided to enable work
(ii) Accessories such as chargers, mouse, pen drives and hard disks
(iii) Shared devices such as printers, scanners, shredders and copiers
(iv) Communication devices such as video conferencing system

(v) Software and applications such as operating system(s), accounting, payroll, ERP, time, and attendance
(vi) Decision of brand, make and specification of IT assets are business and policy driven decisions, and individual preferences will not be entertained.
(vii) IT assets are to be used only for authorized and permitted activities.
(viii) Sahita personnel shall enable regular upgrades and updates (software and hardware), schedule maintenance, and use necessary tools like anti-virus software and firewalls as prescribed by the IT Department.
(ix) IT assets may be required by the IT Department for centralized data backup, installation of policy governance tools, recovery tools and other such purposes. Sahita personnel shall ensure cooperation and timely compliance.
(x) Sahita personnel shall implement all scheduled backups and shall not unreasonably halt or pause backups.
(xi) Sahita personnel shall not share or change passwords and PINs associated with IT assets unless they have been directed by the IT Department.
(xii) Sahita personnel are expected to provide passwords, PIN and access codes on demand by IT for purposes of maintenance, policy checks and systems audit.
(xiii) No asset can be taken outside the premises (except portable assets assigned so), without the authorization of the IT Department.
(xiv) Sahita personnel are absolutely and unconditionally responsible for the IT assets assigned to them and are liable for any consequence arising from misuse or unauthorized use by them or others.
(xv) Sahita personnel are not authorized to alter the hardware specifications or modify any software or applications without consent from and supervision by the IT Department.
(xvi) Sahita personnel will allow access of the IT assets by the IT Department for random audits or spot checks for policy compliance.
(xvii) Use of IT assets for access to sites which are considered to be injurious, suspicious or unsafe and access for personal entertainment may be restricted or regulated as the need may be depending on the policy, role or function of the personnel.
(xviii) Sahita is not responsible for any personal data or monetary loss in transactions, carried out during personal use with the IT asset. For example, net-banking and utilities payments.
(xix) In case of damage or compromise in the functioning ability of the asset, the IT Department would make a comprehensive assessment of the cause and if the cause is found to be mismanagement or inappropriate usage, the concerned personnel may be required to contribute to the cost of repair, replacement or service if needed, based on the severity. This is also applicable in case of loss/theft of the asset.
(xx) Sahita personnel must report any performance issues, physical issues (repairs), software issues, malfunction, damage, unexpected performance with the asset immediately to the IT Department.
(xxi) Sahita personnel must not attempt to repair on their own or have unauthorized personnel fix, repair, modify or restore the IT asset.
(xxii) Sahita personnel are expected to handover all IT Assets in working condition immediately upon demand or upon resignation/termination from employment.

Emails

(i) Sahita personnel are expected to use only official and authorized email IDs.
(ii) Use of personal emails for accessing, sharing or transmitting Confidential Information or Highly Confidential Information is not permitted.
(iii) Use of personal emails will be at the own risk of the personnel. Sahita shall not be responsible for any risk, loss or damage arising out of personal mail access use. Sahita will have the right to take appropriate action for any theft, loss, misuse, damage, destruction and unauthorised access of Sahita information because of use of personal emails.
(iv) Email passwords shall not be shared with others unless it is a shared mail ID or group ID.
(v) Profiles and account information of emails, software, utilities etc. cannot be edited without approval of the IT Department. Personal emails cannot be provided as recovery emails.
(vi) Sahita Personnel must refrain from:

(a) sending emails that may be considered as intimidating, harassing, or offensive. This includes, but is not limited to abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, colour, sex, age, religion, sexual orientation, national origin, or disability;
(b) accessing any website, downloading any program, accessing and public wireless network or use any other device, that could affect or impair, temporarily or permanently, the security of electronic devices used dedicatedly or temporarily for work-related purposes;
(c) using e-mail for the purpose of sending spam emails;
(d) violating copyright laws by illegally distributing protected works;
(e) sending e-mails using another person's e-mail account, except when authorized to send messages for another;
(f) creating a false identity to transmit, share or access any Sahita Information;
(g) forging or attempting to forge e-mail software;
(h) using unauthorized e-mail software;
(i) knowingly disabling the automatic scanning of attachments on any Sahita system or circumventing e-mail security measures;
(j) sending unsolicited messages to large groups, except as required to conduct Sahita business; and
(k) knowingly sending or forwarding email with computer viruses.

Cybersecurity incidents

(i) If you become aware of any Cybersecurity Incident, please report to the IT Department immediately.
(ii) The IT Department is responsible for the mandatory reporting of incidents listed in the directions issued by the CERT-In on 28 April 2022 within six (6) hours of noticing or being brought to notice by any Sahita personnel. The list of Cybersecurity Incidents is also provided as Appendix – A to this policy (the list of cybersecurity incidents are subject to amendment from time to time).

Miscellaneous

(i) The IT Department along with other employees, workers or consultants, must endeavour to conduct periodic information security risk assessment process to identify business-critical (information and non-information) assets, procedures, processes, vulnerabilities, and risks to establish a risk acceptance criterion and operational policies.
(ii) The IT Department shall set the encryption standards to be followed by all Sahita personnel.
(iii) Any deviation from the Policy must be reported to the IT Department.
(iv) Sahita will provide trainings and periodic information awareness regarding this policy.
(v) In case of failure to comply with this policy, Sahita may take any action as it may deem fit as per internal policies and procedures including but not limited to seizure of assets, termination of employment and legal action.
(vi) This policy is effective from [April 1st 2025].

Appendix - A

Types of cyber security incidents that needs to be reported to CERT-ln*:

Targeted scanning/probing of critical networks/systems

Compromise of critical systems/information

Unauthorised access of IT systems/data

Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.

Malicious code attacks such as spreading of virus/worm/Trojan/Botnets/Spyware

Attacks on servers such as Database, Mail and DNS and network devices such as Routers

Identity Theft, spoofing and phishing attacks

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks

Attacks on Critical infrastructure, SCADA Systems and Wireless networks

Attacks on Applications such as E-Governance, E-Commerce etc.

Data breach

Data leak

Fake mobile apps

Unauthorised access of social media accounts and

Attacks or malicious/ suspicious activities affecting artificial intelligence, machine learning, Big Data, blockchain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing, and drones.

(*The list of cybersecurity incidents are subject to amendment from time to time)

****

Appendix - B

Information Classification Policy

Public Information refers to the information that is made available to the general public or information that has been approved for public disclosure. This includes marketing materials, press releases, job announcements, or information that is made available on publicly available websites and over email communications.

Confidential Information refers to information that is not Public Information, and which may relate to / include –

Sahita's business and commercial information,

business and commercial information of its suppliers, customers and business partners, and

internal information intended for restricted / unrestricted use within the Sahita and is not available for public disclosure without prior authorisation such as personnel directories, internal policies and procedures, internal correspondence, draft reports, summaries, minutes of meetings, or information generally obtained from or shared using Sahita's internal networks, systems, or servers.

Disclosure of this information may adversely affect Sahita's interests or market reputation, individual's privacy, interests or reputation of Sahita's supplies, customers or business partners, or attract any legal or regulatory liabilities.

Examples: financial data, customer data, revenue forecasts, intellectual property, contracts, employee information and information subject to non-disclosure agreements.

Highly Confidential Information refers to information that may cause material or significant harm to Sahita or its customers, business partners, employees, or others. This category includes –

personal data of Sahita's directors, employees, agents, consultant, interns and workers,

personal data of directors, employees, agents, consultant, interns and workers of Sahita's suppliers, customers and business partners, strategic plans and proposals, encrypted data, and data relating to encryption methods adopted and used by Sahita.

******