Cyber Security Policy

Context & Scope

Context: Sustana produces sustainable, premium recycled fiber and paper. We work with leading brands, corporations, and customers to create environmentally friendly, sustainable solutions for their packaging and printed material needs and utilize post-consumer material to create high-quality, low carbon products. Our facilities, operations, and personnel, as well as the majority of our customers and suppliers, are located in the United States and Canada.

Scope: This policy applies to Sustana, all its subsidiaries and all its employees and other entities working on behalf of Sustana, including contractors and sub-contractors, volunteers and to all people who have access temporarily or permanently to any of our systems hardware and software components, on premises, or in the cloud.

Summary and Objectives

Sustana's cyber security policy (information technology policy) defines the guidelines and measures taken to preserve and safeguard our information technology (IT) infrastructure and our data security and confidentiality.

As we rely more on technology to collect, store, and manage business information, we become more and more exposed to cyber risks and security or confidentiality breaches. Human errors, cyber attacks and system malfunctions could become the cause of serious financial and reputational damage to our company.

For these reasons, Sustana has elaborated several security measures that lay ground for a more secure cyber environment. We have also prepared general policies and instructions to help reduce our cyber risks.

Basic Cyber Security Policy Elements

- Personally identifiable and/or confidential data
- Clean desk policy
- Enterprise devices protection
- Automatic device protection and controls
- Email protection measures
- Password management rules
- Secure data transfers
- Hacking, suspect activity and confidentiality breaches watch & reporting
- Usage of AI tools
- Additional security measures

- Remote work considerations and policies
- Employee security governance
- Disciplinary measures

Personally Identifiable and/or Confidential Information and Data

Personally identifiable and confidential information and data is precious and must remain confidential. Common personal identifiable information (PII) and confidential data examples include:

- Unpublished or confidential financial company or personal information
- Client / business partners / supplier data
- New technologies, patents and product composition or formulas
- Customer listings (existing and potential clients)
- Any employee or management PII
- Any corporate information which publication could damage the enterprise reputation.

All employees and assimilated are expected to protect computerized data and company information. There are several common measures that should be applied to avoid compromising data security. Cyber pirates and other criminals are more and more organized, and we often face threats from organized crime and state sponsored hackers. At the same time, personal threats and cyber attacks are becoming more common, and we have many examples of these trends within affiliated companies and competitors alike. It is therefore imperative to be vigilant and to participate in the protection of the personal and confidential data you have access to, whether it means your own personal information, or customer, supplier, and partner information that you may have access to. As a company we carry a responsibility to protect PII, as well as any confidential data that we possess or carry on our systems. When it comes to data security, we all carry and share this responsibility as a group, in particular regarding third party and business partners data security.

Clean Desk Policy

To help with personal and confidential data protection we ask all of our employees and system users to refrain from leaving any document which would include personal or confidential data in plain sight on their desk or on their computer screen.

All your desktop systems, Windows/Mac/Android computers, portables, mobile phones, or tablets, should be secured in sleep mode or lock mode when you are not present. Put your systems in lock or sleep mode when you walk away from your desk. By default, and when possible, the corporate policy will force your systems to lock down or sleep after 10 minutes.

Protect Enterprise Devices

Employees are not allowed to use their personal digital devices to access corporate emails or systems. Access to e-mail and other systems like MS teams via personal devices is only allowed if sanctioned by management and IT and only via the secure methods IT recommends.

We strongly advise to protect your company computers, tablets and mobile phones using the following methods (same applies to any personal devices which is used for sanctioned company access):

- Protect your devices with passwords, Sustana enforces secure password management.
- Do not leave your devices exposed or unattended.
- Install browser security updates. Sustana enforces compulsory device updates, but you can choose to delay their run times as convenient.
- Connect to your accounts only using secure networks and encryption methods. Sustana enforces VPN (Virtual Private Network) and MFA (Multi-Factor Authentication) for all remote accesses to corporate systems.

It is strongly advised not to access corporate systems and internal accounts using third party devices, and it is strongly advised not to lend your own devices to other people.

Your personal mobile phone should not be charged via the USB port of your computer, please use only the company supplied electrical power outlet.

Employees are forbidden to install and/or use any unapproved software or hardware which would not be designated as a professional usage on company supplied devices.

Automatic Device Protection

All Sustana devices used for a professional purpose, whether they are company supplied or personal devices, must be carrying standard company security software, which will be supplied and installed automatically on the first connection to the Enterprise networks.

For company supplied systems, some restrictions regarding software or hardware installations may apply, and some security updates will apply regularly and automatically. If you receive a message asking you to confirm an automatic update of your system, be sure to verify that the message comes from a legitimate source before you confirm. Our system triggered automated updates never ask for a password on your behalf, nor do they require any personal information to be disclosed You can only differ an automatic update to a later timeframe if it is not convenient for you at the time it pops up. If you wish to install a particular software or hardware on your company device which is not in our list of employee onboarding approved elements, you will have to contact our IT support department and make a formal request, either via the support portal or via a direct telephone call to the help desk line.

Protect Your Emails

Email messages carry more and more spam messages and phishing attempts as well as malicious software links (like worms). To avoid infecting your computer devices and possibly the enterprise network we ask our employees to be vigilant:

- Avoid opening attachments and clicking on html links when the content is not explicitly described, and always verify the actual email address of the sender rather than its displayed name (for instance a subject such as <look at this incredible video> is suspect).
- Beware of eye-catching links (for instance, price offer, free advice, or download).
- Always check where the email comes from (@domain name) and ensure the person is known to you.
- Look for inconsistencies in the message editing (for instance orthography, use of capital letters, excessive number of exclamation marks).
- Signal any suspect email to IT support by email or via the web support portal Cyber Incident option or call the IT support help desk hotline.
- Employees are not allowed to use text messaging (SMS via mobile phones) to run the corporation business.

If an employee has doubts about a received email legitimacy, he can always refer to Sustana's IT support team.

Cyber Security Awareness Program

From time to time, you could receive unsolicited email messages or phone calls which will come from our IT department Cyber Awareness test platform. Tests like these will be conducted on a regular basis during the year by the IT department to evaluate and reinforce our collective ability to manage phishing and vishing threats. These are simulations of true incidents that commonly happen in the industry and these campaigns are being used to measure our collective degree of awareness to the common threats which circulate on the internet, social media and through corporate networks.

Following these evaluations, Sustana's IT department will then offer targeted cyber security training and coaching, and you may be contacted and get an offer to improve your cyber security awareness abilities through one of these companies' sponsored programs.

Manage Your Password Properly

Password leaks are quite common in any organization but can be very damaging and eventually compromise our whole IT infrastructure. Passwords must not only be secured, in order to avoid being hacked, they must also remain secret and have a minimum degree of complexity. For these reasons we ask our employees to follow these rules:

- Choose passwords with a minimum length of 12 characters (use at least three of the following four groups, i.e.: capital letters, lower case letters, digits and symbols) and avoid easy to guess schemes such as your date of birth or pet's name.

- Change passwords at least once a year. Sustana may have more stringent requirements (e.g., 90 days for key systems).
- Avoid using public networks to enter your company credentials to log into corporate systems and networks, and always check to see if someone is looking over your shoulder.
- Never confirm an approval request for a connection or log onto your Microsoft authenticator app if you did not request this connection yourself. If you have been assigned the responsibility to approve connections on behalf of an external supplier or partner you work with to allow him to connect remotely to our systems, you must ensure first that the request actually comes from the designated authorized person or representative. If not sure, validate by a telephone call to this partner to make sure he is actually the person who requested the connection.

Securely Transfer Your Data

Company data transfers always carry a security risk. Employees transferring data must follow these rules:

- Any confidential information shall not be transferred externally, nor to private e-mail addresses. Only if the transfer of confidential information is sanctioned by management, the transfer to a third party via secure channels is allowed.
- For any data transfer, in particular nominative or confidential data (for instance, customer related information, employee files) towards other devices or to external accounts or systems use only the sharing and transfer tools that have been approved by the company (for instance keeper security vault). The use of external service such as Dropbox, Box, etc. must be approved by the IT department prior to its use on a case-by-case basis.
- When you share data, in particular confidential data, you must be using the enterprise networks and not a public Wifi or network, or even an external private connection without additional security measures as provided by IT (like VPN and MFA).
- Always make sure that the addressee (person or organization) to whom you are sending the data, are duly authorized and have the necessary security and data protection measures themselves.
- Prefer a secure encrypted share link for sending an email to share sensitive content.
- Never send access credentials and passwords via email.
- When in doubt, contact IT which can provide you with the necessary tools and training.

Signal any Scams, Private Info Divulgation and Hacking Attempts

To protect our collective cyber infrastructure, the IT department must be informed as soon as you encounter scams, phishing emails, privacy violations, company network usage violations, or suspect a malware software contamination. We advise all our employees to advise our IT support desk as soon as they feel their data security, integrity or privacy may have been tampered with. Our IT department will quickly inquire and detect any actual threat and will remedy it and possibly send appropriate alerts to the enterprise level if necessary.

Our security specialists can advise on the best ways to detect and dispose of fraudulent emails, malicious software and worms, we invite our employees to contact them for any concern or question regarding cyber security.

Additional Measures

To reduce the probability of security breaches, employees are asked to:

- Put their screens in sleep or lock mode when they go away from their desks.
- Signal any IT equipment theft or damage to the IT support department.
- Modify all their account's passwords in case of theft of a device.
- Signal any perceived threat to or possible security flaw in enterprise systems they use.
- Refrain from installing suspicious, illegal, or unapproved software on any enterprise hardware or virtual or non-virtual IT.
- Refrain from accessing suspicious, illegal, or unauthorized web sites.
- Signal any suspect activity that you may notice around your area.

Employees must not, in any case, conduct activities or behave on enterprise networks in a way that affects directly or indirectly the availability or performance of our enterprise cyber resources. For instance, the sending of nonprofessional emails, like chain emails, subscribing to an excessive number of personal, nonbusiness related mailing lists, playing online games, watching nonbusiness related videos, or streaming channels, allowing the use of 'Peer to Peer' networks or computing, or any other activity which may result in an excessive network traffic or unusual computing activity is prohibited. Our IT professionals monitor the enterprise network traffic constantly, do not expose yourself to illegal or unauthorized behavior by accessing to prohibited web sites or conducting prohibited activities.

Usage of AI Tools

The usage of Artificial Intelligence (AI) tools like ChatGPT and others can add value if used properly. When using AI tools, no confidential information shall be used for facilitating the AI tool, only publicly available Sustana information shall be used. Any non-public or confidential information would become publicly available if used in the context of AI tools.

Remote Working Employees

Employees who benefit of the privilege to work remotely, must also conform to all the rules defined in this policy. As they remotely access to enterprise accounts and systems, remote workers must follow all encryption and data protection rules and must ensure that the networks they use are secure and private. Any remote connection to Enterprise networks must be implemented through a VPN configuration. The access must be approved by your immediate supervisor or manager, and the connection must be protected by one of our company's approved multi-factor authentication methods.

Ask your immediate supervisor or your IT support department for advice and more information.

Never Overlook Security

All of our customers, partners, employees and sub-contractors must be assured that our employees and our company apply state of the art protocols and measures to guarantee the security of the personal and/or confidential data they trust us with. The only way to be worthy of their confidence is to protect our systems and databases using state of the art procedures and technologies. All employees can contribute by staying vigilant and keeping security in mind when performing regular business activities.

Disciplinary Measures

The violation of this policy may generate disciplinary measures that could eventually lead to an employee layoff. Unintentional violations may just lead to a verbal warning, while frequent violations of a similar nature may conduct to a more formal written warning. Intentional violations may eventually lead to employee suspension or work contract cancelation, according to circumstances related to each case.

Reporting

Any violations, concerns or questions regarding this policy and compliance should be reported promptly through appropriate channels by any Sustana employees or third parties to the IT department or management.

Governance

This policy has been edited by the Vice President Information Technology (VP IT) and is supported and has been approved by Sustana's Chief Executive Officer, Chief Commercial Officer and Chief HR Officer. The VP IT shall review this policy annually to make continuous improvements to our security effort and update this policy based on lessons learned, insights, and best practices.

Communication and Transparency

This policy shall be made publicly available on Sustana's website and shared with all employees.

Legal Disclaimers

Sustana reserves the right to modify this policy at its discretion. Updated policies will be shared in a timely manner.

Effective: August 01, 2023

Action	Major Revisions and Comments (if any)	Version and Date
First Edition	First version drafted by Vice President IT, and reviewed by the CEO, CCO and Chief HR Officer.	Version 1.0 August 01, 2023

Fabian de Armas
Chairman & CEO, Sustana

I hereby acknowledge the reading, understanding and acceptance, of the Sustana cyber security procedures and dispositions as contained and defined in this document (Version 1.0 as of August 01, 2023).

_____ _____

Signature Date (MM-DD-YYYY)

_____

Name in capital letters