CYBER SECURITY POLICY

Document details	
Document Name	Cyber Security Policy
Document Version	1.0
Valid from	01.08.2025
Responsible Unit	Information Technology
Responsible Person	Information Security Officer
Approval	

PURPOSE

Styrenix Performance Materials Limited (referred as "**SPML**" or "the Company") recognizes information as a critical business asset. The Company's ability to operate competitively in global markets and meet all its stakeholders evolving requirements depending on the ability to ensure that confidentiality, integrity & availability of its information is protected through pertinent security controls and proactive measures.

Cyber Security Policy ("**the Policy**") provides an integrated set of protection measures that must be uniformly applied across the Company to ensure a secured operating environment for its business operations. Customer Information, organizational information, supporting IT systems, processes and people that are generating, storing, and retrieving information are important assets of the Company. The availability, integrity and confidentiality of information are essential in building and maintaining competitive edge, cash flow, profitability, legal compliance, and respected company image.

The Policy addresses the information security requirements of:

- Confidentiality: Protecting sensitive information from disclosure to unauthorized individuals or systems.
- Integrity: Safeguarding the accuracy, completeness, and timeliness of information.
- Availability: Ensuring that information and vital services are accessible to authorized users when. required.

SCOPE

- The policy applies to all staff, assignees and contractors that provide services to the Company and is an integral part of the SPML's Business Code of Conduct.
- The policy covers the security of information systems and data networks owned or used by the Company as well as the information that is stored, transmitted, or processed by those systems.
- The policy does not cover issues related to general physical and building security. It covers, however, physical security aspects of buildings or parts of buildings that directly affect the security of information owned by the Company.

1. POLICY FRAMEWORK

This policy is intended to help the user to make the best use of the computer resources at their disposal, while minimizing the cyber security risks. The user should understand the following:

- They are individually responsible for protecting the equipment, software, and information to which they have access. Security is everyone's responsibility.
- Identify which data is non-public, which includes company confidential data, client data and personal data as further described below. If the user does not know or is not sure, then they must check with their immediate superior. Even though the user cannot touch it, information is an asset, sometimes a priceless asset.
- Use the resources made available only for the benefit of the Company.
- They are accountable for what they do on the system.
- They should protect equipment from loss & theft.
- only store company data on encrypted devices.
- They should not copy or store the Company's data on external devices or unauthorized external locations (including cloud-based services which are not company approved services). Contact IT for the best solution for secured file transfer when it is required.
- They should not bypass established network and internet access connection rules.
- They should not bypass or uninstall virus protection or firewall software.
- They should not change or install any unauthorized software or browser 'plug-ins'.
- If they become aware of a potential or actual Security Incident then they must report the incident as soon as possible.

2. POLICY CONTENT

2.1 Data Protection

SPML takes the protection of personal data seriously and the security measures set forth in this policy are essential to ensure the data protection standards are met.

2.2 System Access Policy

Access to information and systems in the possession of, or under the control of the Company must be provided based on a least privilege, need to know basis. All the Company's computers must be protected by approved password-based access control systems. Multi-factor authentication for remote access to corporate and production networks by employees, administrators and third parties shall be implemented where available. The following rules must be maintained for managing user access rights:

- User registration: approving and granting access rights to users on a need-to-know basis.
- Privilege management: Clear hierarchies must be determined for each system and each hierarchy must be formally approved.
- User management: As above, each system must have clear procedures for approval and method of granting access to that system. Procedures must exist for each system for both joiners, movers, and leavers, with audit trails.
- User access rights are subject to periodic reviews.
- Inactive user accounts must be disable after 45 days.

2.3 User Authentication Standard

- Users will be forced to change their passwords during the first log on and at 60-day intervals.
- Passwords shall not be displayed or transmitted in clear text and shall be suitably protected via approved cryptographic solutions. Passwords shall be stored in an encrypted format. A history of passwords shall be maintained to prevent the re-use of passwords. A maximum of six successive login failures shall result in account lockout until an administrator unlocks it. Default accounts shall be disabled and / or default passwords associated with such accounts shall be changed.

2.4 Acceptable Use Policy

Corporate IT resources may only be used for SPML's business related purposes.

➢ *Email Usage*

E-mail is a business communication tool which all the employees are requested to use in a responsible, effective, and lawful manner.

➢ *Internet Usage*

The Company provides Internet access to all staff to assist them in carrying out their duties such as looking up details about suppliers, products, accessing governmental information and other work-related information. Occasional and limited personal use of the Internet is permitted if such use does not:

- Interfere with work performance & productivity.
- Include downloading or distribution of large files.
- Have negative impact on the performance of SPML's IT systems.

When using Internet access facilities, the user should comply with the following guidelines:

- Personal use of Internet must be kept to a minimum.
- Check that any information used from the Internet is accurate, complete, and current.
- Respect the legal protections of data, software, copyright, and licenses.
- Immediately inform the Security team in case of any unusual occurrence.
- Do not download or transmit text or images which contain any software, material of obscene, threatening, racist or extreme political nature or which incites violence, hatred, or any illegal activity
- Do not use the company's equipment to make unauthorized access to any other computer or network.
- The Company reserves the right to inspect and erase portable media that is used on its network.

➢ *Portable Media*

- The use of portable media is not permitted.
- The intended purpose is to protect customer and company information from being transferred via unauthorized means
- Do not use the company's equipment to make unauthorized access to any other computer or network.
- Portable Media will be permitted in case of business requirement only after the Approval.

2.5 Remote Access and Electronic Communication

Frequently users will be required to access the Group's Information systems from outside the office, for example travelling consultants and / or employees working in Sales / Business Solutions.

For remote access to the Corporate IT Infrastructure resources only the officially supported and approved facilities by the internal IT department are to be used (i.e., SPML Secure Access Portal). The associated security policies must be applied.

Online Communication within SPML offices to an external party may only use the Company's approved communication channels. Personal internet connections or connectivity devices (e.g., using personal data modems and Mobile Hotspot connections, remote access connections, personal VPNs etc.) are strictly prohibited.

2.6 System Changes and Configuration

The Company recognizes that change is a necessary process in order that we can maintain, protect, and enhance services provided to clients, however uncontrolled change can create significant security risks for the Company.

The Company also recognizes that there are different types of change, therefore, an efficient change management process must be implemented to handle these different types in the most appropriate manner.

All changes must be conducted in a controlled and approved way, in accordance with the IT Change Management Standard and IT System Configuration Standard. System changes or re-configurations of standard IT components are not allowed. Only additions and / or changes of software components can be made by users on workstations based on customer project requirements.

The following system changes are strictly prohibited.

- *Installation of:*
  - Unauthorized connectivity devices (e.g., data modems).
  - Any component suitable to gain unauthorized access to restricted areas.
  - Any other non-standard software or hardware component.
- *Merging of two networks by physically integrating them on a network node.*
- *Disabling virus protection.*

2.7 Network & Communication Policy

- *Internet Usage*

At SPML, a secure network is critical to the security of our business:

- External facing networks should be firewalled to an appropriate level.

- Appropriate controls should be in place at network interfaces.
- WAN services should only be acquired through approved vendors.
- Third-party users shall not connect their computing devices to the wired or wireless network of SPML, unless authorized.
- The Company's computers and networks may be connected to third-party computers or networks only with explicit approval after determination that the combined systems are complied with company's security requirements.

➢ *Wireless Networks*

- Passwords for Guest wireless networks should be changed on a regular basis.
- Only approved wireless access points should be used.
- Wireless networks should always be encrypted.

2.8 Workstation Security

Workstations include laptops and desktops:

- All workstations should have corporate-approved antivirus software installed and enabled.
- All workstations should have data loss protection software installed (where available).
- All laptops should be encrypted.
- Only install software from trusted sources.
- Do not allow unauthorized users to access your workstation.
- Take appropriate steps to maintain the physical security of your workstation.

2.9 Mobile Device Security

- Mobile devices capable of accessing the Company's information shall be enrolled in the company Mobile Device Management Solution.
- In the event of the loss of a mobile device or unauthorized access to a mobile device, the user should contact the local IT team and report the Security Incident to the Information Security Team.

2.10 Bring Your Own Device

- Only SPML owned devices are considered trusted and can be connected directly to the Company's Local Area Network (LAN). All non-SPML owned devices are by default considered as untrusted.

- Untrusted devices must never be connected directly to SPML Internal network, neither through a network cable connection in the office, nor through the Employee wireless network.

- Untrusted (non-SPML owned) devices are only allowed to use Visitor network access while in office. Employees personal devices are not allowed to be connected to the Company's corporate network.

2.11 Encryption

- Encryption is required to be used to protect Company non-public Information from being disclosed to unauthorized parties.

- All personnel are responsible for assessing the confidentiality level of data being sent or residing on the devices they use. If data is non-public, all the employees are responsible to comply with the Encryption Standard.

2.12 Security Waivers

Security Policies and Standards are developed to provide the company with a set of rules to help meet certain organizational objectives. From time to time there will be a need to consider a time-limited waiver for exceptions to policy, these will only be considered through the Information Risk Acceptance Standard.

3. RESPONSIBILITY

Styrenix Performance Materials Limited's digital and information systems and all e-mail, voice mail and text messages and all other information and data created by transmitted through or stored in these systems, are and will remain always the exclusive property of the Company.

- All the employees and external parties as defined in policy are responsible to ensure the confidentiality, integrity, and availability of the company's information assets.

3.1 All Staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. All staff should understand:

- What information they are using, how it should be used, stored, and transferred in terms of data security.

- What procedures, standards and protocols exist for the sharing of information with other parties.
- How to report a suspected breach of information security within the organization.
- Their responsibility for raising any information security concerns.

3.2 External Contractors

- All contracts with external contractors that allow access to the organization's data or information. systems must be in operation before access is allowed.
- These contracts must ensure that the staff or sub-contractors of the external organization comply with all appropriate security policies.

4. PERIODIC REVIEW

- The policy shall be reviewed ***every three years or at the time of any major change in existing IT environment affecting policy and procedures.***
- The policy shall also be reviewed to ensure its alignment to the business needs, evolving threat landscape & all applicable regulatory requirements and such revisions shall be communicated to all concerned.

5. BREACH OF POLICY

Breach of this Policy will be taken seriously and may result in disciplinary actions in conformity with the legal and contractual framework, including termination of employment. Any user disregarding the rules set out in this Policy or in applicable laws will be fully liable and the Company will disassociate itself from the user as far as legally possible. All breaches of this policy must be reported to the respective Manager / Director for appropriate action. All security incidents, whether actual or suspected, must be reported as soon as possible.

6. AMENDMENTS

Amendments from time to time to the Policy, if any, shall be considered by the Board of Directors of the Company. Any amendments in the applicable law, including any clarifications / circulars of relevant regulator, if mandatory, shall be read into this policy such that the policy shall automatically reflect the
contemporaneous applicable law at the time of its implementation. The company reserves the right to modify this policy at any time.