Cyber Security Policy

Version: 1.1

Effective date: October 27, 2025

Owner: Jamie Saveall (VP Operations, ESG & Compliance Lead)

Review cycle: Annual

Policy Brief & Purpose: Stratavor's Cyber Security Policy outlines our approach to preserving the security of the Company's data and technology infrastructure. As a technology-driven company, we recognize that relying on digital systems comes with vulnerabilities – threats such as human error, cyber-attacks, or system failures could cause financial loss or damage our reputation. Therefore, Stratavor has implemented a number of security measures and provides guidance to mitigate these risks. This policy serves to inform all personnel of their responsibilities in maintaining cyber security and to establish protocols for protecting our information assets.

Scope: This policy applies to all Stratavor staff and partners who have access to our systems or data, including employees, contractors, interns, freelancers, and any third parties with whom we share systems access. It covers all devices (company-issued or personal devices used for work), all IT systems, cloud services, software applications, and data located on or handled through Stratavor's network.

Policy Elements: The following key elements form the basis of Stratavor's cyber security measures:

- **Confidential Data Handling:** All confidential data must be treated as sensitive and protected. Examples of confidential information include, but are not limited to: unpublished financial information, customer or partner data, proprietary business

plans, source code, and client list. Every team member is obligated to protect such data. This means not disclosing it to unauthorized persons, storing it securely (e.g., using encryption), and only retaining it as long as necessary.

- **Device Security:** When using any digital devices (laptops, smartphones, tablets) to conduct Stratavor business or access company accounts, staff must follow strict security practices. This includes:
    - Keeping all devices password-protected with strong, unique passwords or passphrases.
    - Installing and regularly updating reputable antivirus/anti-malware software on devices.
    - Applying all security patches and system/software updates in a timely manner (at least monthly, or as soon as critical updates are available).
    - Ensuring devices are not left unattended in unsecured locations; use screen lock and physically secure devices when not in use.
    - Not using personal devices for work unless they meet Stratavor's security standards and are authorized. Avoid accessing company systems from public or untrusted devices.
- **Network Security:** Access to Stratavor's internal systems and accounts should only occur over secure networks. Employees and contractors must:
    - Use secure, private networks or a trusted VPN when accessing company resources remotely. Public Wi-Fi networks should be avoided or used only in conjunction with a VPN.
    - Not create insecure network hotspots or share network access with unauthorized users.
    - Ensure that any Wi-Fi network used for work (e.g., home network) is secured with strong encryption (WPA2/WPA3) and a strong router password.

- **Account Security:** All accounts (email, internal tools, cloud services) must be protected:
    - **Strong Authentication:** Use strong passwords and enable multi-factor authentication (MFA) on all Stratavor accounts wherever possible. MFA adds an extra layer (such as a phone app code) to prevent unauthorized access even if a password is compromised.
    - **Access Controls:** Access to systems is granted on a need-to-use basis. Employees should only have access to the data and systems required for their role. Higher-privilege accounts (like admin accounts) are limited to authorized personnel and used sparingly.
    - **Credential Management:** Never share passwords or authentication tokens. Do not reuse Stratavor passwords on other services. If you suspect any account credentials are compromised, notify IT/security personnel immediately and change the password.
- **Data Transfer & Storage:** When transferring or storing data, precautions must be taken to preserve security:
    - Use encrypted communication channels for sensitive data (for instance, ensure websites use HTTPS; use encrypted file transfer methods for confidential files).
    - Avoid sending sensitive information over email or messaging unless absolutely necessary and encrypted (consider using secure file-sharing links with access controls).
    - Store data in Stratavor-approved cloud storage or databases that have proper security measures; avoid unapproved personal cloud accounts for company data.

    - Classify data (public, internal, confidential) and handle it according to its classification. Highly sensitive data might have extra restrictions (e.g., not downloadable to personal devices).

- Physical Security: For any Stratavor hardware (like laptops or external drives), keep them secure. Lock laptops when not in use; in public places, never leave them unattended. Documents containing sensitive info, if printed, should be stored securely and shredded when no longer needed.
- Software Use: Only use authorized and licensed software for company work. Do not install unapproved software on company systems as it may contain vulnerabilities or malware. All software should be kept updated. Be cautious of downloading attachments or clicking links – verify the source to avoid phishing.

Incident Reporting: All staff must be vigilant and immediately report any suspected cyber security incidents or weaknesses. This includes lost or stolen devices, suspicious emails (possible phishing), unexpected system behavior, or any possibility that confidential data has been compromised. Report incidents to as soon as discovered. Quick reporting allows us to take containment measures to minimize damage.

Incident Response: Stratavor has procedures in place to respond to security incidents. Upon report of a potential breach or incident, we will investigate promptly, mitigate any security threats, inform affected parties as required, and take steps to prevent recurrence. Where required by law (such as certain data breaches under GDPR or other regulations), we will notify authorities and individuals whose data might be affected.

Business Continuity: We perform regular backups of critical data to secure, off-site locations to ensure business continuity in case of a cyber incident or outage. Employees should save work on approved cloud storage that is backed up. In the event of a system failure or attack (like ransomware), we have recovery procedures to restore operations from backups with minimal data loss.

Employee Responsibilities: Cyber security is everyone's responsibility. Each Stratavor team member must:

- Adhere to the guidelines set in this policy and complete any required security awareness training.
- Exercise good judgment online – for example, do not open attachments or click on links from unknown senders (to prevent phishing and malware).
- Keep personal use of Stratavor devices or accounts to a minimum and ensure it does not introduce risks.
- When in doubt about a security matter, ask our IT/Security team for guidance.

Management Responsibilities: Stratavor's management will support strong cyber security by providing necessary tools, training, and enforcement of this policy. We will regularly assess risks and update security measures accordingly. Management will also conduct periodic audits or reviews of compliance with cyber security practices.

Disciplinary Action: Violations of this Cyber Security Policy (e.g., deliberate breach of data security, negligence leading to a breach, or ignoring security protocols) may result in disciplinary action. Depending on severity, consequences range from additional training and warnings up to termination of contract or legal action if laws were broken. Our aim is not to punish accidental mistakes but to prevent incidents; however, reckless or intentional disregard for security is taken very seriously.

Review and Updates: This policy will be reviewed at least biannually and updated as needed to address emerging threats, new technologies, or changes in Stratavor's IT environment. We stay informed about the latest cyber security trends and adapt our policies to ensure ongoing protection.

By following this Cyber Security Policy, Stratavor and its personnel work together to create a secure digital environment, protecting our data assets and maintaining the trust of our clients and stakeholders.