VERAXUS LTD
CYBER SECURITY POLICY

DATE: 02/05/2026

VERAXUS LTD
GENERAL CONTRACTORS

DATA PROTECTION
We protect the confidentiality, integrity, and availability of all data.[cite: 2]

THREAT PREVENTION
We defend against hacking, ransomware, phishing, and breaches.[cite: 2]

LEGAL COMPLIANCE
We ensure full adherence to UK GDPR and data protection laws.[2]

CLEAR RESPONSIBILITIES
We define explicit duties for employees, IT, and third parties.[cite: 2]

CYBER AWARENESS
We foster a strong, proactive security culture across all teams.[cite: 2]

VIGILANT DEFENSE. SECURE SYSTEMS. TRUSTED PARTNERSHIPS.[cite: 1]

1. Purpose

The purpose of this Cyber Security Policy is to establish a comprehensive framework for protecting Veraxus Ltd's information systems, digital assets, and data from cyber threats, unauthorized access, loss, or damage. As a construction company, Veraxus Ltd processes and stores sensitive project information, financial records, employee data, and client and supplier details that must be protected throughout their lifecycle. This policy sets out the minimum security standards and behaviours expected when using company systems, handling information, and working with third parties. It also defines how Veraxus Ltd will prevent, detect, respond to, and recover from cybersecurity incidents to support safe and reliable operations.

Policy Objectives

- **Safeguard confidentiality, integrity, and availability (CIA) of information:** Confidentiality means information is only accessible to authorized people and systems; integrity means information remains accurate, complete, and protected from unauthorized change; availability means information and systems are accessible when needed to support business operations (e.g., project delivery, payroll, and invoicing).
- **Protect against internal and external cyber threats:** This includes threats such as phishing (fraudulent messages designed to steal credentials or money), ransomware (malware that encrypts files and demands payment), business email compromise (impersonation to redirect payments), malware and trojans (malicious software that steals data or provides remote access), credential stuffing (reuse of leaked passwords), insider threats (intentional or accidental misuse), and denial-of-service attacks (disruption of services). Controls include secure configuration, patching, access controls, monitoring, and user awareness.
- **Meet legal and regulatory compliance requirements:** Veraxus Ltd will process personal data in line with the UK GDPR and the Data Protection Act 2018, including principles such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. Security measures will be proportionate to risk and will support rights of data subjects, breach management, and appropriate record-keeping.
- **Define responsibilities and accountability:** Clear responsibilities ensure security tasks are owned, performed consistently, and verified. This reduces gaps in controls, supports effective decision-making during incidents, and ensures that employees, contractors, and suppliers understand what is required of them when handling Veraxus Ltd information and systems.
- **Promote a culture of security awareness:** Veraxus Ltd will build awareness through onboarding, mandatory training, regular reminders, simulated phishing where appropriate, clear reporting routes, and leadership support. A "report early" culture is encouraged so potential issues can be contained quickly without blame for good-faith reporting.

By implementing and maintaining these controls, Veraxus Ltd aims to reduce operational disruption, financial loss, regulatory exposure, and reputational damage. Strong

cybersecurity also supports safe project delivery by protecting schedules, designs, and communications from tampering or loss. Consistent application of this policy helps maintain trust with clients, suppliers, employees, and other stakeholders.

2. Scope

This policy applies to all individuals, devices, systems, and information assets that create, access, store, transmit, or process Veraxus Ltd data. It applies regardless of whether work is performed on company premises, at construction sites, or remotely, and regardless of whether systems are hosted on-site or in approved cloud services.

Personnel Coverage

- **Full-time and part-time employees:** Must follow this policy at all times, use company systems responsibly, protect credentials, complete required training, and report suspected incidents immediately. Access is granted based on role and business need and may be monitored for security and compliance purposes.
- **Temporary staff and interns:** Must follow the same security rules as employees but will typically receive limited access aligned to their duties. Access will be time-bound, supervised where appropriate, and removed promptly at the end of the engagement. Temporary personnel must not use personal email accounts or unapproved tools to store or share company information.
- **Contractors and subcontractors:** Must meet Veraxus Ltd security requirements when accessing sites, systems, or information (including project documentation and communications). Third parties must use approved channels for data exchange, protect any data shared with them, and comply with contractual security clauses, including incident reporting and confidentiality obligations.
- **Consultants and third-party service providers:** Vendors providing IT, cloud, payroll, finance, design, or other services must be managed through vendor due diligence and contractual controls. They must implement appropriate technical and organisational measures, restrict access to authorized personnel, and support audits, incident response, and data protection obligations where applicable.

Data Types Covered

- **Project documentation (drawings, plans, contracts, schedules):** Often commercially sensitive and may include site layouts, security details, and contractual terms. These documents must be stored in approved repositories, shared on a need-to-know basis, and protected from unauthorized modification to preserve integrity and safety.
- **Financial records (invoices, payment details, banking information):** Must be treated as confidential and protected against fraud and unauthorized disclosure. Payment instructions must be verified using approved processes to reduce the risk of business email compromise and invoice redirection scams.
- **Employee and HR data:** Includes personal data such as contact details, payroll information, right-to-work documentation, and performance records. This data must be processed in line with UK GDPR and the Data Protection Act 2018, with strict access controls and secure retention and disposal.

- **Client and supplier information:** Includes contact details, contracts, pricing, and communications. Protecting this information supports relationship management, confidentiality commitments, and compliance obligations, and reduces the risk of impersonation and fraud.
- **Email and communication records:** Includes emails, messages, meeting notes, and attachments. These records may contain personal data and commercially sensitive information and must be retained, archived, and disposed of in line with business needs, legal requirements, and approved retention schedules.

Devices and Systems

- **Company-issued devices (laptops, desktops, mobiles, tablets):** Must be configured and managed to company standards, including security updates, endpoint protection, encryption where applicable, and monitoring for threats. Users must not disable security controls or install unapproved software.
- **Personal devices (BYOD – Bring Your Own Device):** May only be used for work where explicitly permitted and must meet minimum security requirements (e.g., device lock, supported OS versions, and separation of company data). Veraxus Ltd may restrict access, require security controls, and remove company data if a device is lost, stolen, or the user leaves.
- **Cloud platforms and storage systems:** Only approved services may be used to store or process company data. Cloud services must meet security and contractual requirements, including access controls, encryption, logging, and appropriate data residency/sovereignty considerations where relevant to client or regulatory requirements.
- **Email systems and collaboration tools:** Must be used securely, with appropriate sharing permissions, careful handling of links and attachments, and adherence to retention and acceptable use requirements. Sensitive information must not be shared via unapproved channels or personal accounts.

Locations

- **Office environments:** Office networks and devices must be protected through secure Wi-Fi configuration, strong authentication, controlled physical access, and secure printing and disposal practices. Visitors must not be given unsupervised access to systems or confidential information.
- **Construction sites:** Sites present additional physical and digital risks (shared spaces, temporary offices, variable connectivity, and higher risk of device loss). Personnel must secure devices, avoid using unknown USB devices, use approved connectivity methods, and protect printed documents and site records from unauthorized access.
- **Remote working environments:** Remote access must use secure connections (e.g., VPN where required), strong authentication (including MFA), and approved devices. Users must avoid public/shared computers, secure home Wi-Fi (e.g., strong router password and encryption), and prevent shoulder-surfing or unauthorized viewing of sensitive information.

3. Responsibilities

Cybersecurity is a shared responsibility across Veraxus Ltd. Effective security depends on consistent behaviours, clear ownership of controls, and timely reporting of issues. All personnel must actively contribute to maintaining a secure environment and protecting company and personal data.

Management Responsibilities

- **Implementation and maintenance:** Ensure appropriate security controls are implemented, documented, and maintained across the business, including oversight of third-party services where they support company operations.
- **Resource allocation:** Provide sufficient budget and resources for security tools, secure configurations, monitoring, backups, and training, proportionate to business risk and legal obligations.
- **Policy enforcement:** Enforce compliance through clear expectations, fair disciplinary procedures, and consistent action when policy breaches occur, including corrective actions and retraining where needed.
- **Incident response leadership:** Provide leadership during major incidents, including decision-making on containment, business continuity, communications, and engagement with external support (e.g., insurers, legal counsel, or specialist responders).
- **Regular review and updates:** Sponsor periodic reviews of this policy and related procedures to ensure continuous improvement, alignment with changing threats, and compliance with legal and contractual requirements.

Employee Responsibilities

- **Follow cybersecurity best practices:** Examples include locking screens when away, verifying payment requests, using approved storage and sharing tools, and checking recipients before sending sensitive information.

- **Protect credentials and access:** Use strong, unique passwords, enable MFA where required, never share accounts, and immediately report suspected credential compromise or unusual login prompts.
- **Report incidents promptly:** Report suspected phishing, lost devices, malware warnings, misdirected emails, or any suspected data breach immediately in line with the incident reporting procedure. Early reporting reduces impact and supports legal timelines.
- **Use systems for authorized purposes only:** Follow acceptable use boundaries, avoid unapproved software and services, and do not attempt to bypass security controls. Access and use must align with job responsibilities and business needs.
- **Participate in training:** Complete mandatory training on time, apply learning in day-to-day work, and cooperate with security awareness activities (e.g., policy acknowledgements and periodic refreshers).

IT/System Administrator Responsibilities

- **System security maintenance:** Maintain secure configurations, apply operating system and application patches, manage vulnerabilities, and ensure supported versions are used. Critical security updates should be prioritised and deployed within defined timelines based on risk.
- **Network monitoring and threat detection:** Monitor logs and alerts, investigate suspicious activity, and maintain appropriate detection capabilities (e.g., endpoint protection alerts, email security alerts, and access logs).
- **Access control implementation:** Implement role-based access controls, enforce least privilege, manage joiner/mover/leaver processes, and ensure privileged access is tightly controlled and audited.
- **Backup and recovery management:** Ensure backups are performed, protected, and tested; maintain recovery procedures; and support restoration during incidents or operational failures.
- **Security tool deployment:** Deploy and maintain security tools such as antivirus/anti-malware, firewalls, device encryption, email filtering, and mobile/device management controls where applicable.

Third-Party Responsibilities

- **Compliance requirements:** Third parties must comply with Veraxus Ltd security requirements and any contractual clauses relating to confidentiality, data protection, and secure processing.
- **Data protection standards:** Suppliers must implement appropriate technical and organisational measures (e.g., access controls, encryption, secure development/operations practices) to protect Veraxus Ltd data and prevent unauthorized access or disclosure.
- **Incident reporting obligations:** Third parties must notify Veraxus Ltd promptly of any incident that may affect Veraxus Ltd systems or data, including suspected breaches, service compromises, or loss of data, and must cooperate with investigation and remediation.
- **Audit cooperation:** Where contractually required, third parties must provide reasonable assurance (e.g., security questionnaires, certifications, or audit evidence) and support

verification of controls relevant to the services provided.

Failure to comply with this policy may result in disciplinary action (up to and including dismissal), termination of contracts, removal of system access, and/or legal consequences. Veraxus Ltd may also be required to report certain incidents or breaches to regulators, clients, or other parties where legally or contractually required.

4. Data Protection

Veraxus Ltd is committed to ensuring that all data is handled securely and in compliance with applicable laws, regulations, and contractual obligations. Data protection is achieved through classification, secure handling, controlled access, secure storage, and defined retention and disposal processes.

Data Classification System

- **Confidential:** Highly sensitive information such as financial data, payroll, employee records, client contracts, and security-related information. Access is restricted to authorized roles only, sharing must be controlled, and additional protections (e.g., encryption and logging) should be applied where appropriate.
- **Internal:** Information intended for internal business use such as project documents, internal procedures, and operational communications. This data should not be shared externally without approval and must be stored in approved systems with appropriate access controls.
- **Public:** Information approved for public release such as marketing materials and published company information. Public data must still be accurate, approved, and protected from unauthorized modification to prevent reputational harm.

Data Handling Requirements

- **Authorized access only:** Access to sensitive data must be limited to individuals with a legitimate business need. Identity and access should be verified through unique user accounts, strong authentication, and approval workflows for higher-risk access.
- **Encryption standards:** Encryption should be used to protect sensitive data in transit (e.g., secure email methods, HTTPS, VPN, secure file transfer) and at rest where appropriate (e.g., device encryption, encrypted storage). Encryption keys and credentials must be protected and managed securely.
- **Physical document security:** Printed confidential documents must be stored securely (e.g., locked cabinets), not left unattended on desks or in vehicles, and disposed of using secure methods (e.g., cross-cut shredding or approved confidential waste services).
- **Transmission security:** Sensitive files must be shared using approved secure methods (e.g., controlled-access links, secure portals, or encrypted attachments where approved). Avoid sending sensitive data to personal email accounts or via unapproved messaging apps.

Access Control Principles

- **Approved storage systems:** Company data must be stored in approved systems such as managed file shares, approved cloud storage, and business applications with access controls and audit logging where appropriate.
- **Prohibited storage methods:** Unauthorized storage (e.g., personal USB drives, personal cloud accounts, or unapproved external hard drives) is prohibited unless explicitly approved for a defined business need with appropriate safeguards. These methods increase the risk of loss, malware infection, and uncontrolled sharing.
- **Cloud storage policies:** Cloud providers must be approved and meet security requirements such as encryption, access controls, logging, and contractual commitments. Data residency/sovereignty requirements must be considered where client contracts or regulations require it.
- **Mobile device storage:** Sensitive data should not be stored permanently on mobile devices unless necessary and protected (e.g., encryption, secure containers, and remote wipe capability). Where possible, access should be via secure apps rather than local downloads.

Data Retention and Disposal

- **Retention schedules:** Data must be retained only as long as necessary for business, legal, regulatory, and contractual purposes. Retention periods should be defined by data type (e.g., HR records, financial records, project documentation) and reviewed periodically.
- **Secure deletion methods:** When data is no longer required, it must be securely deleted using appropriate methods (e.g., secure erase for devices, controlled deletion for cloud storage, and secure disposal for physical media). Simple deletion (e.g., “recycle bin”) may not be sufficient for sensitive data.
- **Documentation requirements:** Where required, disposal actions should be recorded (e.g., destruction certificates for confidential waste, device disposal records, or deletion logs) to support accountability and compliance.

5. Password Policy

Strong password practices are essential to preventing unauthorized access to Veraxus Ltd systems and data. Passwords are a primary control for protecting accounts, and weak or reused passwords significantly increase the risk of compromise through phishing, credential stuffing, and brute-force attacks.

Password Complexity Requirements

- **Minimum length:** Passwords must be at least 8–12 characters, with a strong recommendation of 12+ characters for improved security. Longer passphrases (e.g., three or more unrelated words) are encouraged where supported.
- **Character composition:** Passwords should include a mix of uppercase and lowercase letters, numbers, and special characters where supported. Example: a passphrase with added complexity (e.g., “River!Stone7Window”) is stronger than a short complex string.
- **Prohibited passwords:** Do not use common passwords, dictionary words, predictable patterns (e.g., “Password123!”), or personal information (e.g., names, birthdays, company name, project names). These are easily guessed or found in leaked password lists.

Password Management Best Practices

- **No sharing:** Passwords must not be shared with anyone, including colleagues, managers, or third parties. If access is required, it must be provided through proper account provisioning or delegated access. Shared credentials reduce accountability and increase breach risk.
- **Unique passwords:** Passwords must not be reused across multiple systems. Reuse enables credential stuffing attacks, where attackers try leaked passwords from other services to access company accounts.
- **Regular changes:** Passwords should be changed immediately if compromise is suspected, after a phishing incident, or when instructed due to a security event. Routine forced changes should be risk-based and aligned with system capabilities and guidance.
- **Default password changes:** Default passwords on devices, applications, or accounts must be changed immediately upon setup. Default credentials are widely known and frequently exploited.

Multi-Factor Authentication (MFA)

- **What MFA is:** MFA requires two or more factors to sign in (something you know, something you have, or something you are). This reduces the risk of account compromise even if a password is stolen.
- **Where to enable:** MFA must be enabled for email accounts, remote access/VPN, cloud services, collaboration tools, and any system that stores or provides access to confidential data, where technically feasible.
- **MFA methods:** Preferred methods include authenticator apps or hardware tokens. SMS-based MFA may be used where other methods are not available but is generally less secure than app- or token-based methods.

- **Benefits:** MFA provides an additional security layer against phishing, password reuse, and brute-force attacks and is a key control for protecting high-value accounts.

Password Storage and Management

- **Prohibited practices:** Passwords must not be written down in unsecured locations, stored in plain text files, or shared via email or messaging apps. These practices create easy opportunities for theft and misuse.
- **Password managers:** Use of approved password managers is encouraged to generate and store strong, unique passwords securely. Access to password managers must be protected with a strong master password and MFA where available.
- **Browser password storage:** Storing passwords in browsers may be restricted depending on device controls and risk. Where permitted, it must be protected by device security controls and should not be used for high-risk administrative accounts unless approved.

6. Device Security

All devices used for company work must be secured to prevent unauthorized access, data loss, and malware infection. Device security controls protect Veraxus Ltd information whether devices are used in the office, on construction sites, or remotely.

General Device Requirements

- **Lock screen protection:** Devices must be protected with a password, PIN, or biometric lock. Shared devices should be avoided; where unavoidable, access must still be controlled and logged where possible.
- **Automatic locking:** Automatic screen locking must be enabled with an appropriate timeout (e.g., 5–10 minutes) to reduce the risk of unauthorized access when devices are unattended.
- **Physical security:** Devices must not be left unattended in unsecured locations (e.g., vehicles, open site cabins). When travelling, devices should be kept with the user or stored securely. Confidential documents should not be left visible.
- **Device registration:** Company-issued devices must be recorded in an inventory and assigned to a user. Where BYOD is permitted, devices may need to be registered to enable security controls and access management.

Software and Update Management

- **Operating system updates:** Operating systems must be kept up to date using automatic updates where possible. Unsupported or end-of-life operating systems must not be used for company work.
- **Application updates:** Applications must be updated regularly to address security vulnerabilities. Users must not delay critical updates without approval.
- **Security patches:** Critical security patches should be applied promptly based on risk (e.g., within days for critical vulnerabilities where exploitation is likely). Patch status should be monitored and exceptions documented.
- **End-of-life software:** Software that is no longer supported by the vendor must be replaced or removed. Continued use increases exposure to known vulnerabilities and

may breach contractual or regulatory expectations.

Antivirus and Malware Protection

- **Approved software:** Approved antivirus/anti-malware protection must be used on company devices. Where centrally managed solutions are available, they must be installed and kept enabled.
- **Installation requirements:** Endpoint protection must not be disabled or removed. Tampering with security controls may result in disciplinary action and immediate removal of device access.
- **Regular scanning:** Devices must run regular scans (scheduled or continuous) and users must report repeated detections or unusual behaviour (e.g., pop-ups, slow performance, unknown programs).
- **Real-time protection:** Real-time monitoring should remain enabled to detect threats as they occur, including malicious downloads and suspicious processes.

Personal Device (BYOD) Policy

- **Security standards:** BYOD devices must meet minimum standards such as supported OS versions, device encryption where available, screen lock, and up-to-date security patches. Rooted/jailbroken devices must not be used for company access.
- **Data storage limitations:** Company data should be accessed through approved apps and should not be stored permanently on personal devices unless explicitly approved. Where possible, containerisation or managed profiles should be used to separate company data from personal data.
- **Company access controls:** Veraxus Ltd may require mobile device management (MDM) or equivalent controls to enforce security settings, manage access, and enable remote wipe of company data if needed.
- **Inspection rights:** Where permitted by law and policy, Veraxus Ltd may perform security checks relevant to company access (e.g., verifying encryption and patch status). These checks are limited to protecting company data and systems.

Lost or Stolen Device Procedures

1. Report immediately to management and/or IT using the approved contact route, providing device details, last known location, and the time the loss was discovered.
2. If available, initiate remote lock and remote wipe procedures as directed by IT to protect company data.
3. Change passwords for accounts accessed on the device (especially email and cloud services) and revoke active sessions where possible.
4. Document the incident, including any suspected unauthorized access, and cooperate with follow-up actions (e.g., police report where appropriate and replacement device provisioning).

7. Email and Phishing

Email is one of the most common attack vectors used to deliver malware, steal credentials, and commit payment fraud. All personnel must treat unexpected messages with caution and

follow secure email practices to reduce the risk of phishing and business email compromise.

Phishing Recognition

- **Suspicious sender addresses:** Attackers may spoof names or use lookalike domains. Verify the full email address and be cautious of slight spelling changes or unusual domains.
- **Unexpected attachments:** Attachments may contain malware or prompt you to enable macros. Treat unexpected invoices, “delivery notes,” or “urgent documents” as suspicious until verified.
- **Urgent or threatening language:** Social engineering often pressures recipients to act quickly (e.g., “payment needed today” or “account will be closed”). Pause and verify through a trusted channel.
- **Requests for sensitive information:** Be cautious of requests for passwords, MFA codes, bank details, or personal data. Legitimate organisations will not ask for passwords or MFA codes by email.
- **Poor grammar and spelling:** Errors, unusual phrasing, or inconsistent branding can indicate fraud, though some sophisticated attacks may appear professional.
- **Suspicious links:** Hover over links to preview the destination and look for mismatched or shortened URLs. Do not sign in via links in unexpected emails; navigate directly to the service instead.

Email Best Practices

- **Link verification:** Hover to preview links and confirm the domain is correct before clicking. When in doubt, access the website by typing the address or using a trusted bookmark.
- **Sender verification:** For payment requests or sensitive changes (e.g., bank detail updates), verify using an independent method such as calling a known number from records (not the email signature).
- **Attachment scanning:** Use endpoint protection and approved tools to scan files. Do not enable macros or run executable files received by email unless explicitly approved and verified.
- **Sensitive information handling:** Do not email sensitive data unless necessary and approved. Use secure sharing methods and encryption where required, and apply least-privilege sharing permissions.

Reporting Procedures

1. Report suspicious emails immediately to IT/management using the approved reporting route (e.g., forwarding as an attachment or using a reporting button if available).
2. Include key details such as the sender address, subject line, time received, and why it appears suspicious (e.g., unusual link, payment request, unexpected attachment).
3. If you clicked a link, opened an attachment, or entered credentials, report this immediately and do not attempt to “fix it yourself.” Prompt reporting enables rapid containment.
4. Do not respond to, reply-all, or engage with suspected phishing attempts. Engagement can confirm your address is active and may increase targeting.

Email Attachments and Links

- **Trusted sources only:** Only open attachments and links from trusted, verified sources. If the message is unexpected, verify with the sender through a known contact method.
- **File scanning:** Scan files where possible and ensure endpoint protection is active. Report repeated detections or suspicious file behaviour immediately.
- **Compressed files:** Treat ZIP/RAR and password-protected archives as higher risk because they can conceal malicious content. Only open if verified and required for business purposes.
- **Executable files:** Do not open or run executable attachments (e.g., .exe, .js, .bat) received by email. These are commonly used to deliver malware and are generally prohibited.

8. Backup and Recovery

Data backup is critical for business continuity and protection against cyberattacks, accidental deletion, hardware failure, and ransomware. Backups enable Veraxus Ltd to restore systems and data to a known good state and reduce downtime and financial impact.

Backup Requirements

- **Backup frequency:** Backups must be performed regularly based on data criticality (e.g., daily for core business systems and active project data; weekly for less frequently changing data). Frequency should be reviewed as business needs change.
- **Data coverage:** Backups must include critical business data such as project repositories, finance systems, HR records, email where applicable, and key configuration data required to rebuild systems.
- **Backup verification:** Backups must be verified through integrity checks and monitoring to confirm they complete successfully and are usable for restoration.

- **Backup documentation:** Backup jobs, schedules, failures, and corrective actions must be logged to support accountability and audit requirements.

Backup Storage

- **Multiple locations (3-2-1 rule):** Where feasible, maintain at least three copies of data, on two different media types, with one copy stored off-site/offline to reduce the risk of a single event compromising all backups.
- **Local backups:** Local backups can support fast restoration but must be secured, access-controlled, and protected from malware spread from production systems.
- **Cloud backups:** Cloud backups provide off-site redundancy and should be configured with strong access controls, encryption, and logging. Access to backup consoles must be restricted and protected with MFA.
- **Physical security:** Backup media (if used) must be stored securely, protected from theft, fire, and water damage, and handled through controlled processes with tracking where appropriate.

Backup Testing

- **Regular testing schedule:** Backups must be tested periodically (e.g., quarterly for critical systems and at least annually for others) to confirm data can be restored within required timeframes.
- **Restoration procedures:** Conduct recovery drills to validate steps, responsibilities, and dependencies (e.g., credentials, encryption keys, and system rebuild requirements).
- **Documentation:** Record test results, issues found, and remediation actions. Update recovery procedures based on lessons learned.

Ransomware Protection

- **Backup isolation:** Backups must be isolated from main systems to reduce the risk of ransomware encrypting or deleting backup data. Use separate credentials and restricted network paths where possible.
- **Immutable backups:** Where supported, use immutable or write-once storage features to prevent alteration or deletion of backups for a defined retention period.
- **Version retention:** Maintain multiple restore points so data can be recovered from a time before compromise, including protection against “slow” ransomware or delayed detection.
- **Recovery planning:** Recovery plans should align with business continuity needs, including prioritisation of critical systems and clear decision-making processes during an incident.

9. Incident Response

A structured incident response is essential to minimise damage, restore operations quickly, and meet legal and contractual obligations. Veraxus Ltd will respond to incidents in a controlled manner to contain threats, preserve evidence, and reduce the likelihood of recurrence.

Incident Definition and Types

- **Data breaches:** Unauthorized access, disclosure, alteration, or loss of personal data or confidential business information (e.g., misdirected emails containing personal data, stolen devices with unencrypted data, or compromised cloud accounts).
- **Malware infections:** Malicious software such as ransomware, trojans, spyware, or keyloggers that can encrypt files, steal data, or provide attackers with remote access.
- **Unauthorized access:** Account compromise, privilege escalation, or access by individuals without permission (e.g., shared credentials, stolen passwords, or misuse of admin rights).
- **System outages caused by cyber events:** Disruptions due to attacks or security failures (e.g., denial-of-service, destructive malware, or compromised infrastructure).
- **Phishing attacks (successful compromise):** Incidents where phishing leads to credential theft, fraudulent payments, malware execution, or unauthorized mailbox rules and forwarding.

Reporting Procedures

1. **Who to contact:** Report immediately to your line manager and the designated IT support/provider. If IT support is unavailable, escalate to senior management without delay.
2. **Information to provide:** Describe what happened, when it was discovered, systems/accounts involved, actions already taken, and any evidence (e.g., screenshots, email headers, filenames, error messages).
3. **Timing requirements:** Report immediately upon suspicion—do not wait for confirmation. Early reporting supports containment and helps meet legal timelines for breach assessment and notification.
4. **Documentation:** Complete any required incident form or record, and preserve relevant evidence (do not delete emails or logs unless instructed).

Response Actions

1. **Containment:** Isolate affected devices or accounts (e.g., disconnect from network, disable compromised accounts, block malicious domains) to prevent further spread or data loss.
2. **Assessment:** Determine the scope and impact, including what data or systems are affected, whether personal data is involved, and whether the threat is ongoing.
3. **Eradication:** Remove malicious components, close vulnerabilities, reset credentials, and apply patches or configuration changes to prevent re-entry.
4. **Recovery:** Restore systems and data from clean backups, validate system integrity, and monitor for recurrence. Recovery should prioritise critical business services.
5. **Communication:** Coordinate internal and external communications to stakeholders as appropriate, ensuring messages are accurate, timely, and approved by management and relevant advisors.

Investigation and Analysis

- **Incident documentation:** Maintain a clear record of actions taken, timelines, affected assets, and evidence collected. Preserve logs and relevant artefacts to support forensic analysis where needed.
- **Root cause analysis:** Identify how the incident occurred (e.g., phishing, unpatched vulnerability, misconfiguration, weak access controls) and what control failures contributed.
- **Lessons learned:** Conduct a post-incident review to identify improvements in processes, training, tooling, and technical controls.
- **Preventive measures:** Implement corrective actions such as patching, configuration hardening, improved monitoring, updated procedures, and targeted training to reduce recurrence risk.

Legal and Regulatory Reporting

- **GDPR notification timelines:** Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, Veraxus Ltd must assess and, where required, notify the relevant authority without undue delay and, where feasible, within 72 hours of becoming aware of the breach.
- **ICO reporting:** In the UK, reportable personal data breaches may need to be notified to the Information Commissioner's Office (ICO). Decisions and rationale (including when not reporting) must be documented.
- **Client and stakeholder notification:** Where required by law, contract, or risk assessment, affected clients, suppliers, or individuals may need to be informed with clear guidance on protective steps.
- **Documentation:** Maintain records of breach assessments, decisions, notifications, and remediation actions to demonstrate compliance and support audits or investigations.

10. Training and Awareness

Mandatory Training

All personnel must complete cybersecurity and data protection training as part of onboarding and at regular intervals thereafter. Training must cover core topics such as phishing awareness, password and MFA practices, safe data handling, device security, and incident reporting. Completion may be tracked, and failure to complete mandatory training may result in restricted access to systems until training is completed.

Ongoing Awareness

Veraxus Ltd will maintain ongoing awareness activities such as periodic reminders, security bulletins, posters or site briefings, and targeted communications during heightened threat periods (e.g., known phishing campaigns). Where appropriate, simulated phishing exercises may be used to reinforce safe behaviours and identify areas for additional support. Awareness materials will be tailored to construction and site-based realities, including safe handling of devices and documents in shared environments.

Specialized Training

Role-based training will be provided for higher-risk roles such as finance (payment verification and fraud prevention), HR (handling special category data and privacy obligations), project management (secure sharing and access control), and IT/administrators (secure configuration, monitoring, and incident response). Additional training may be required when new systems are introduced or when incidents indicate a need for targeted improvement.

11. Policy Review and Updates

Review schedule

This policy will be reviewed at least annually to ensure it remains effective, practical, and aligned with current threats, business operations, and legal requirements.

Trigger events

Additional reviews will be conducted when significant changes occur, including changes in legislation or regulatory guidance, introduction of new systems or technologies, major changes to business operations or suppliers, or following a cybersecurity incident or near miss.

Update communication

Updates will be communicated to all relevant personnel through appropriate channels (e.g., email announcements, intranet postings, team briefings, and site communications). Where changes affect third parties, relevant contractual or operational communications will be issued to ensure continued compliance.

Electronic Approval & Signature

Document: Cyber Security Policy

Reference: Document date: 02/05/2026

Approved and signed electronically on behalf of Veraxus Ltd

This document has been electronically approved and signed by the Director of Veraxus Ltd. The typed signature below is intended to authenticate and approve this document on behalf of the company. This approval applies to the attached policy document for normal company policy, supplier registration, website and tender-support use.

Name	Alex Stefan
Position	Director
Signature	Alex Stefan
Date	08 May 2026

Electronic approval block added for Veraxus Ltd policy documentation.