CYBER SECURITY POLICY

A practical policy for protecting Veraxus Ltd systems, accounts, project records, communications and commercially sensitive information.

Company	Status	Effective date	Next review
Veraxus Ltd	Approved	08 May 2026	08 May 2027, or earlier if required

POLICY AT A GLANCE

Secure systems Accounts, devices, cloud storage, email and project records are protected using proportionate technical and organisational controls.	**Controlled access** Access is based on role, business need and least privilege, with strong passwords and MFA used where available.
Fraud and threat prevention Phishing, invoice redirection, ransomware, malware, unauthorised sharing and lost-device risks are actively managed.	**Fast reporting and recovery** Personnel are expected to report concerns early so incidents can be contained, assessed, recorded and corrected quickly.

CONTENTS

Controlled copy note:
This document may be issued as a controlled PDF for client assurance, tender submissions, website download, internal governance and professional stakeholder review. Where a later signed copy is issued, the later signed copy takes precedence.

Publication note:
The website presentation version may summarise this policy in plain language, but this official policy remains the controlled reference document for formal client, tender and governance use.

Guidance alignment:
This policy has been rebuilt with reference to official UK guidance and recognised control themes, including ICO data security and breach guidance, UK GDPR and Data Protection Act 2018, NCSC Cyber Essentials and NCSC small organisation cyber security guidance.

Document use	Practical meaning
Client and tender assurance	Demonstrates that Veraxus Ltd applies controlled, proportionate cyber security governance when handling project, client, supplier, finance and business records.
Internal governance	Sets expected behaviours for account protection, document control, email caution, secure sharing, device care, backup and incident reporting.
Plain-language summary	Keep systems secure, restrict access to those who need it, verify suspicious requests, back up important records and report concerns early.

PRACTICAL OPERATING STANDARD

Control point	Expected practical behaviour
Project records	Store tender, quotation, RAMS, programme, site photograph, snagging and handover records in controlled business locations.
Payment requests	Check new payees, bank detail changes and urgent payment instructions through independent known contact routes before action.
Access and sharing	Use least privilege, controlled links and approved systems so sensitive information is not exposed unnecessarily.
Reporting culture	Report suspicious emails, lost devices, wrong-recipient disclosures and unusual account activity early so action can be taken.

1. INTRODUCTION

1.1 Responsible digital working: Veraxus Ltd recognises that cyber security is part of professional project control, not a separate technical exercise. Drawings, quotations, contracts, invoices, emails, photographs, site notes and payment instructions can all carry operational, commercial or personal risk if handled carelessly.

1.2 Construction and refurbishment context: The company may work with clients, principal contractors, subcontractors, suppliers, professional advisers, finance providers and site-based teams. Cyber security therefore supports safe communication, clear document control, payment protection, confidentiality, business continuity and trusted delivery.

1.3 Practical and proportionate controls: This policy sets a clear baseline for day-to-day security behaviours, account protection, device security, approved systems, incident reporting and supplier controls. Controls are applied in a way that is proportionate to company size, business activity, client requirements and the sensitivity of the information involved.

2. PURPOSE OF THIS POLICY

The purpose of this policy is to provide a practical framework for preventing, detecting, responding to and recovering from cyber security risks affecting Veraxus Ltd operations.

- **Confidentiality:** protect sensitive information from unauthorised access, disclosure or misuse.
- **Integrity:** keep records accurate, complete and protected against unauthorised alteration.
- **Availability:** maintain access to important systems and project records when required for business operations.
- **Fraud prevention:** reduce the risk of phishing, invoice redirection, business email compromise and impersonation.
- **Client assurance:** demonstrate responsible governance suitable for commercial, residential, landlord, insurance and public sector environments.

Policy position
This policy forms part of Veraxus Ltd wider compliance and operational governance framework. It supports confidentiality, data protection, tender readiness, project administration, safe communications and responsible use of digital systems.

3. LEGISLATIVE AND GUIDANCE FRAMEWORK

Veraxus Ltd will apply cyber security controls in a way that supports relevant legal, regulatory, contractual and client assurance requirements. The company will consider recognised UK guidance where appropriate, while keeping the policy practical and proportionate for the business.

Reference area	How it informs this policy
UK GDPR and Data Protection Act 2018	Security controls support appropriate protection of personal data, breach assessment, accountability and secure handling.
ICO data security and breach guidance	The policy supports appropriate technical and organisational measures, early reporting, breach records and risk-based decision-making.
NCSC Cyber Essentials	Control themes include firewalls, secure configuration, user access control, malware protection and security update management.
NCSC small organisation guidance	Practical controls include backing up data, protecting devices, securing email, protecting online accounts and spotting attacks.
Contracts and tender requirements	Client, principal contractor, public-sector portal or professional adviser requirements may add project-specific obligations.

Reference basis
This policy is not a technical certification statement. It is an approved company policy that sets baseline governance and practical controls. Where a client or scheme requires certification, questionnaire evidence or technical audit, Veraxus Ltd will assess that requirement separately.

4. SCOPE OF THIS POLICY

This policy applies to people, systems, devices and information used to create, access, store, share or process Veraxus Ltd business data. It applies whether work is carried out from an office, home environment, construction site, client premises, vehicle, supplier location or approved cloud platform.

Scope area	Application
People covered	Directors, employees, workers, temporary staff, contractors, subcontractors, consultants, professional advisers and third parties who access Veraxus Ltd systems or information.
Information covered	Project records, tenders, quotations, contracts, drawings, RAMS, site photographs, emails, payment details, HR records, supplier records and commercially sensitive information.
Systems covered	Email, cloud storage, collaboration tools, finance systems, website administration, mobile devices, laptops, tablets, removable media and approved business applications.
Locations covered	Office, remote working, vehicles, construction sites, site cabins, client premises and any other location where company information is accessed or stored.

Practical scope test
If information relates to a Veraxus Ltd project, quotation, client, supplier, employee, payment, site record, tender, commercial arrangement or company system, it should be handled as controlled business information unless it has been approved for public release.

5. KEY TERMS

Cyber security: Controls and behaviours used to protect systems, accounts, devices, networks, data and communications from unauthorised access, disruption, fraud or damage.
Information asset: Any record, file, system, account, device or dataset that has value to the business or its stakeholders.
MFA: Multi-factor authentication, requiring more than one form of verification before access is granted.
Phishing: Fraudulent messages designed to steal information, credentials, money or access to systems.
Business email compromise: Impersonation or account compromise used to redirect payments, change bank details or obtain sensitive information.
Incident: An event that may affect confidentiality, integrity, availability, privacy, payments, systems or business continuity.
Personal data breach: A security incident that leads to accidental or unlawful loss, destruction, alteration, disclosure of, or access to, personal data.

6. GOVERNANCE AND RESPONSIBILITIES

Directors / management Approve this policy, allocate proportionate resources, maintain oversight, enforce expectations, lead major incident decisions and ensure review. As the business grows, management will improve systems, controls and evidence.	**Employees and workers** Use systems responsibly, protect credentials, check recipients and payment requests, avoid unapproved tools, keep devices secure, complete training and report concerns promptly.

IT support / system administrators Maintain secure configuration, access controls, patching, backup processes, endpoint protection, monitoring, account setup and technical response where appointed or engaged.	**Suppliers and subcontractors** Protect information shared with them, use agreed communication routes, maintain confidentiality, report relevant incidents and follow project-specific security or data-handling requirements.

Accountability note
Cyber security is a shared responsibility. Management sets the standard, but every person handling Veraxus Ltd information must apply common-sense security, question unusual requests and report concerns early.

7. INFORMATION ASSETS AND DATA CLASSIFICATION

Veraxus Ltd information should be handled according to sensitivity, business value and potential harm if lost, altered or disclosed. Classification supports proportionate controls rather than unnecessary complexity.

Classification	Examples	Minimum handling standard
Confidential	Financial records, bank details, payroll, HR records, client contracts, tender pricing, supplier rates, passwords, security information and commercially sensitive project records.	Need-to-know access, approved systems, careful sharing, MFA where available, secure retention and controlled disposal.
Internal	Working project notes, draft documents, supplier coordination, non-public procedures, internal communications and business planning records.	Store in approved systems, avoid public sharing, check recipients and keep access aligned to business need.
Public	Approved website content, published policies, marketing wording, public contact details and formally released company information.	Ensure information is accurate, approved for release and protected against unauthorised alteration.

Information assets covered

- **Project and tender records:** drawings, scopes, specifications, quotations, programmes, RAMS, permits, inspection records, site photographs, snagging evidence and handover records.
- **Financial and commercial records:** invoices, bank details, supplier rates, project pricing, payment instructions, contracts, purchase orders and accounting records.
- **Client and stakeholder information:** contact details, communications, access arrangements, resident or site-user information and commercially sensitive instructions.
- **Business systems and accounts:** email accounts, cloud storage, device accounts, website administration, finance platforms, document systems and collaboration tools.

Document control standard
Company records should be stored so that the current version can be identified, access can be limited, and important evidence is not lost. Where records are issued externally, they should be sent as controlled copies using appropriate file names and permissions.

Data handling and storage controls

Control	Required behaviour
Approved storage	Use approved business storage, email and document platforms. Avoid personal cloud storage, unmanaged USB drives or informal records where controlled storage is available.
Controlled sharing	Share only what is required, with the correct recipient, using suitable permissions or secure transfer methods where sensitivity requires it.
Paper records	Keep confidential paper records secure, avoid leaving documents visible in vehicles or site cabins, and dispose of them by shredding or confidential waste where needed.
Site evidence	Photographs and messages should show the work, condition, defect, instruction, progress or handover point - not unnecessary personal details or private belongings.
Retention and disposal	Retain records for business, legal, contractual, insurance, warranty and evidence purposes only as long as required; then delete, archive, anonymise or destroy in a controlled way.

8. ACCESS CONTROL, PASSWORDS AND MFA

Access to Veraxus Ltd systems must be controlled so that people can only see, use or change information required for their role or approved business purpose.

Control	Required standard
Least privilege	Give users the minimum access needed to perform their role. Higher-risk access should be approved, restricted and reviewed.
Unique accounts	Use individual user accounts wherever possible. Shared credentials must not be used where individual access can reasonably be provided.
Joiner / mover / leaver control	Grant, change or remove access promptly when a person joins, changes role, completes a project or leaves.
Privileged access	Limit administrator access, protect it by MFA where possible, and use it only for administration tasks.
Access review	Management or IT support should periodically review key accounts, cloud permissions, shared folders and external access links.

Password and sign-in requirements

- **Strong passwords or passphrases:** Use long, unique passwords. Passphrases made from unrelated words are encouraged where supported.
- **No reuse:** Do not reuse personal passwords for company systems, and do not reuse company passwords across unrelated services.
- **No sharing:** Passwords, MFA codes and recovery codes must not be shared by email, message or phone. If access is needed, request proper access.
- **Default passwords:** Default passwords on devices, routers, applications or new accounts must be changed before operational use.
- **Risk-based changes:** Passwords must be changed immediately if compromise is suspected, after a phishing event, or when management or IT support instructs a change.

Multi-factor authentication

MFA should be enabled for email, cloud storage, finance systems, remote access, website administration, business applications and any account containing confidential or commercially sensitive information, where available. Authenticator apps or hardware security keys are preferred where practicable; SMS MFA may be used where no stronger option is available.

Access control note
A lost password is inconvenient; a stolen account can affect clients, payments, project records and reputation. For that reason, unusual sign-in prompts, unexpected MFA requests and suspected compromise must be reported immediately.

9. DEVICES, SOFTWARE AND CLOUD SYSTEMS

All devices used for company work must be protected against unauthorised access, malware, loss and accidental disclosure. This applies to company-issued and approved personal devices.

Area	Operating control
Device lock and physical security	Use PIN, password or biometric lock. Do not leave devices or confidential documents unattended in vehicles, site cabins or public areas.
Updates and patching	Keep operating systems, browsers, applications and security tools up to date. Unsupported software should be replaced or removed.
Anti-malware protection	Use approved anti-malware/endpoint protection where available. Security controls must not be disabled without approval.
BYOD and mobile access	Personal devices may be used only where permitted and must have a screen lock, supported operating system and sensible separation of company data.
Cloud systems	Use approved business accounts and controlled sharing permissions. Avoid personal cloud storage for company information.

Site and remote working note
Devices used on sites, in vehicles or away from office environments should be treated as higher risk because of shared spaces, temporary access arrangements and increased risk of loss or theft. Screens and paperwork should be protected from casual viewing.

10. EMAIL, PHISHING AND PAYMENT FRAUD

Email and messaging tools are essential to project delivery, but they are also common routes for fraud, malware, credential theft and accidental disclosure. Personnel must slow down, verify and report when something looks unusual.

Risk indicators and expected response

- **Unexpected attachment or link:** Do not open until verified. Be especially cautious with invoices, delivery notes, zipped files, macros or password-protected archives.
- **Urgent or threatening wording:** Pause and verify. Fraudsters often pressure people to bypass normal checks or act immediately.
- **Bank detail or payment change:** Verify using an independent known contact route, not the phone number or email signature in the new message. Record the check.
- **Lookalike sender or domain:** Check the full email address and domain spelling. Do not rely only on the display name.
- **Request for password, MFA code or sensitive data:** Do not provide it. Report the message to management or IT support.
- **Wrong recipient or accidental disclosure:** Report immediately and do not attempt to hide or delete evidence of the error.

Secure communication rules

- **Check recipients:** Review addresses, attachments and email chains before sending confidential information or client records.
- **Use controlled links:** Where possible, share files through approved platforms with suitable permissions instead of attaching large uncontrolled copies.
- **Avoid personal accounts:** Do not send company files to personal email accounts or informal storage unless specifically approved for a defined business reason.
- **Payment verification:** Bank detail changes, new payees and urgent payment requests must be verified independently and recorded before action.
- **Report early:** If a link was clicked, credentials were entered, an attachment was opened or money may be at risk, report immediately.

Payment fraud control
For Veraxus Ltd, invoice redirection and business email compromise are treated as high-risk threats. A payment instruction is not treated as safe simply because it appears in an email chain or appears to come from a known person.

11. BACKUP, RECOVERY AND BUSINESS CONTINUITY

Backups protect Veraxus Ltd against accidental deletion, hardware failure, ransomware, account compromise and operational disruption. Recovery planning is especially important where project records, quotations, invoices, programme information or handover evidence are needed for ongoing works.

Control area	Expected approach
Backup coverage	Important business data should be backed up, including project folders, finance records, HR records, website/admin records and key communication evidence where applicable.
Backup frequency	Frequency should reflect business need and risk. Active project, finance and operational records should be backed up regularly.
Backup protection	Backups should be access-controlled and, where practicable, separated from main systems so ransomware or accidental deletion does not affect all copies.
Testing	Restoration should be tested periodically so the company knows that backup copies are usable.
Continuity planning	Critical records, contact routes and recovery steps should be documented sufficiently to continue essential business activity during disruption.

12. INCIDENT RESPONSE AND BREACH MANAGEMENT

A structured response reduces damage, supports recovery and helps meet legal or contractual duties. Personnel should report concerns on suspicion, not only after proof is available.

Response stages

- **1. Report:** Tell management and IT support immediately. Provide time discovered, systems affected, what happened and any screenshots, emails, filenames or error messages.
- **2. Contain:** Disconnect affected devices if instructed, disable or reset compromised accounts, revoke sessions and stop further sharing or payment action.
- **3. Assess:** Identify affected systems, accounts, data types, individuals, client records, project records and business impact.
- **4. Recover:** Remove malware, patch weaknesses, restore from clean backups and verify that systems are safe before normal use resumes.
- **5. Record:** Keep an incident record covering facts, decisions, actions, notifications, recovery steps and lessons learned.
- **6. Improve:** Apply corrective action such as training, configuration changes, access review, supplier follow-up or updated procedures.

Examples of incidents to report

- **Phishing or suspicious messages:** including links clicked, attachments opened or credentials entered.
- **Lost or stolen devices:** including phones, laptops, tablets, USB drives or printed documents.
- **Unauthorised access:** unusual sign-in alerts, unexpected MFA prompts, new mailbox rules or unexplained file activity.
- **Malware or ransomware:** warnings, encrypted files, suspicious software, pop-ups or unusual system behaviour.
- **Data breach or misdirection:** emails or files sent to the wrong person, lost records, unauthorised disclosure or accidental deletion.

Personal data breach note
Where an incident may involve personal data, Veraxus Ltd will assess whether notification to the ICO or affected individuals is required. Not every incident is reportable, but incidents should be logged and assessed promptly. Where notification is required, UK GDPR expects reporting without undue delay and, where feasible, within 72 hours of becoming aware.

13. SUPPLIERS AND THIRD-PARTY SYSTEMS

Control area	Veraxus Ltd approach
Due diligence	Select reputable suppliers and systems appropriate to the sensitivity of data and operational reliance involved.
Contractual safeguards	Use confidentiality, data protection, access, incident reporting and service continuity expectations where relevant.
Need-to-know access	Give third parties only the information and access necessary for their role, package or service.
Incident cooperation	Suppliers should promptly notify Veraxus Ltd of incidents that may affect company information, systems or project records.
Exit and removal	Access should be removed when supplier engagement ends or when access is no longer required.

Third-party control note
Where a supplier, subcontractor or professional adviser handles Veraxus Ltd information, the company should consider what is shared, why it is shared, how it is protected and how access will be removed when no longer required.

14. TRAINING, AWARENESS AND MONITORING

Veraxus Ltd will promote practical cyber security awareness through onboarding, reminders, management oversight and lessons learned from incidents, near misses, client requirements and changing threats.

Awareness area	Expected coverage
Onboarding	Basic cyber security, acceptable use, passwords, MFA, phishing awareness, secure sharing and incident reporting.
Role-based reminders	Finance/payment verification, project evidence handling, supplier control, HR records, site photographs and cloud sharing.
Ongoing awareness	Periodic reminders, briefings or updates when threats, systems, projects or client requirements change.
Monitoring	Access logs, sharing permissions, unusual activity, training completion and incident trends may be reviewed proportionately.

Awareness note
Training should not be treated as a tick-box exercise. The practical aim is for people to recognise suspicious requests, protect records, verify payment changes, use approved systems and report concerns before damage grows.

15. POLICY REVIEW AND CONTINUOUS IMPROVEMENT

This policy will be reviewed annually and earlier where required. Review may be triggered by legal or regulatory change, client or tender requirements, operational growth, system changes, supplier changes, incident findings or new cyber threats.

Review trigger	Action expected
Annual review	Confirm that the policy remains suitable for the company's current systems, people, projects and risk profile.
Material incident or near miss	Review the cause, corrective actions and whether policy wording, training or controls need improvement.
New system or supplier	Assess access, data protection, backup, account ownership, continuity and incident reporting arrangements.
Client or tender requirement	Check whether the client requires additional evidence, certification, questionnaires, insurance or project-specific controls.

Review approach
The review is intended to keep the policy practical, proportionate and suitable for Veraxus Ltd construction, refurbishment, tendering, project administration and business governance activities.

Tender and governance evidence

Evidence type	How it may be used
Approved policy PDF	Provided to clients, advisers, contractors, portals and professional stakeholders as evidence of company cyber security governance.
Access and account notes	Used internally to demonstrate that key systems, cloud folders and email accounts are managed with appropriate ownership and permissions.
Backup and continuity checks	Used to confirm that important records can be recovered and that project delivery is not dependent on one uncontrolled device or account.
Incident and improvement log	Used to record suspected incidents, near misses, decisions, reporting assessments and corrective actions.
Supplier controls	Used to show that subcontractors, advisers and service providers are given only relevant information and are expected to protect it.

16. DECLARATION AND ELECTRONIC APPROVAL

This policy is approved by Veraxus Ltd and applies across company operations. It is intended to support responsible cyber security governance, client assurance, tender readiness, internal governance and professional standards.

Approval application

- **Company governance:** The policy sets the expected standard for protecting Veraxus Ltd systems, records, accounts, communications and information assets.
- **Client and tender assurance:** The policy may be issued to clients, advisers, contractors, portals and stakeholders as evidence of controlled cyber security governance.

- **Operational use:** Personnel should use this policy when handling email, cloud storage, passwords, devices, site records, project evidence and payment instructions.
- **Future improvement:** The policy will be reviewed as systems, suppliers, legal duties, tender requirements and business operations develop.

Approval statement: 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.

Approval item	Detail
Name	Alex Stefan
Position	Director
Signature	Alex Stefan
Date	08 May 2026
Document status	Approved
Next review	08 May 2027, or earlier if required
Final control check	**Expected standard**
Complete document	The policy should be issued as a complete PDF so that wording, approval and review information remain together.
No informal edits	Externally issued copies should not be altered without replacing the full controlled policy.
Review trigger	A review should be considered after material system, supplier, tender, legal, operational or incident-related change.
Responsible ownership	Directors retain overall responsibility for ensuring the policy remains suitable for the company's operations.

Approval control note
This approval confirms the policy standard at the date shown. The document should be reviewed when systems, legal requirements, tender requirements, business processes or cyber risks materially change.

Controlled document note
When issued externally, this policy should be treated as a controlled business document. Any future update should be issued as a replacement policy rather than by informal amendment to the signed approval page.

Website and tender use note
A plain-language website summary may be used for visitors, but where a client, adviser or tender portal requires formal evidence, this signed policy PDF should be provided as the authoritative document.

Completion note
This policy has been prepared as a formal, electronically approved document for controlled use by Veraxus Ltd.