
GLOBAL CYBERSECURITY & INFORMATION SECURITY POLICY
Effective Date: 29 October 2025
Last Reviewed: 18 August 2026
Document Status: Public Corporate Cybersecurity Policy
Applies Globally: Subject to applicable local mandatory law

---

1. PURPOSE

Engineering Projects TM LTD ("EPTM LTD") recognises cybersecurity and information security as essential components of responsible architectural, engineering, design, consultancy and project–management operations.

This Policy establishes EPTM LTD's global corporate principles and minimum mandatory security requirements for protecting:

- client information;
- project information;
- engineering information;
- drawings;
- BIM information;
- calculations;
- reports;
- commercial information;
- personal information;
- corporate information;
- intellectual property;
- digital systems;
- communications;
- credentials;
- cloud services.

EPTM LTD shall maintain security measures proportionate to the sensitivity, value, legal obligations and operational importance of information and systems. This Policy establishes the Company's corporate baseline; detailed technical procedures, standards or project–specific security requirements may impose stronger controls where required.

---

2. SCOPE

This Policy applies to:

- employees;
- directors;
- consultants;
- contractors;
- authorised third parties;
- Company systems;

- Company–managed devices;
- cloud services;
- applications;
- project information;
- digital communications.

All persons and third parties within scope shall comply with applicable security requirements and shall protect Company and client information from unauthorised access, use, alteration, disclosure, loss, destruction or disruption.

Project–specific contractual or client security requirements shall be followed where applicable, provided they do not conflict with mandatory law or an authorised Company requirement.

---

3. LEGAL FRAMEWORK

EPTM LTD's cybersecurity approach is principally based on applicable UK requirements, including where applicable:

- UK data–protection legislation;
- Data Protection Act 2018;
- UK GDPR, as amended;
- Data (Use and Access) Act 2025 and applicable commenced provisions;
- Computer Misuse Act 1990;
- Privacy and Electronic Communications Regulations 2003;
- applicable contractual obligations;
- applicable intellectual–property laws;
- applicable confidentiality obligations;
- applicable cybercrime and information–security requirements.

Where other jurisdictions apply mandatory cybersecurity or privacy requirements, EPTM LTD shall comply with those requirements where applicable.

Where a legal, regulatory, contractual or client requirement imposes a higher or more specific security obligation than this Policy, the stricter applicable requirement shall be followed unless prohibited by law.

---

4. INFORMATION CLASSIFICATION

EPTM LTD may classify information according to its sensitivity and business importance.

Information may include:

- **Public** – information authorised for public disclosure;
- **Internal** – information intended for authorised Company use;
- **Confidential** – information whose unauthorised disclosure could adversely affect EPTM LTD, its personnel, clients or third parties;
- **Highly Confidential** – sensitive information requiring enhanced protection;

- **Restricted/Project–Sensitive** – information subject to heightened contractual, client, security, intellectual–property or project requirements.

Information shall be accessed, stored, transmitted, copied and disclosed only as authorised and according to its classification. Highly Confidential and Restricted/Project–Sensitive information shall receive enhanced access, sharing and storage controls appropriate to its risk.

---

5. ACCESS CONTROL

EPTM LTD shall apply, as appropriate to the system and risk:

- least–privilege access;
- role–based access;
- unique user accounts;
- appropriate authentication;
- access reviews;
- prompt removal of unnecessary access.

Access shall be granted only for legitimate business purposes and shall be limited to the minimum permissions required.

Privileged or administrative access shall be separately controlled where technically practicable and shall not be used for ordinary activities.

User access shall be reviewed periodically and following material role changes, termination, suspected compromise or other relevant security events. Access shall be removed or adjusted promptly when no longer required.

---

6. PASSWORDS AND AUTHENTICATION

Users shall:

- use strong, reasonably unique passwords or passphrases;
- avoid password reuse across Company and unrelated services;
- protect credentials from disclosure;
- never share credentials except through an expressly authorised secure mechanism where technically necessary;
- use multi–factor authentication (MFA) for systems supporting MFA, particularly email, cloud services, administrative accounts and other sensitive systems;
- report suspected credential compromise promptly.

Credentials shall not be stored in insecure documents, emails, messages or other readily accessible locations.

Where supported, privileged, administrative and other high–risk accounts shall use enhanced authentication controls.

---

7. DEVICES

Company and authorised devices shall be:

- appropriately secured;
- maintained with supported security updates;
- protected against malware and other reasonably foreseeable threats;
- protected against unauthorised access;
- configured according to business and security requirements.

Security updates shall be applied within a reasonable period appropriate to their risk, with critical security updates prioritised.

Devices containing Company or client information shall use appropriate access protection and, where technically supported and proportionate to risk, encryption.

Lost, stolen, compromised or suspected–compromised devices shall be reported promptly.

---

8. SOFTWARE

Software shall be obtained from legitimate and trustworthy sources and maintained appropriately.

Users must not install unauthorised or malicious software on Company systems.

Software, plugins, extensions, scripts and applications shall be authorised before installation where Company approval is required.

Unsupported, obsolete or materially vulnerable software shall be removed, upgraded or otherwise risk–controlled as reasonably practicable.

Security tools, automated services, AI systems, cloud applications or other external technologies shall not be used to process Company or client information where such use is prohibited by Company requirements, contract, law or applicable security restrictions.

---

9. CLOUD SECURITY

EPTM LTD may use cloud platforms for:

- project files;
- collaboration;
- communications;
- application hosting;
- document management;
- backups;
- business administration.

Cloud services shall be selected and configured with appropriate security considerations and shall, where technically available and proportionate to risk, use:

- MFA and strong authentication;
- least–privilege access;

- appropriate role–based permissions;
- encryption in transit and, where available and appropriate, at rest;
- secure sharing settings;
- restricted external access;
- logging or audit capabilities;
- appropriate backup or recovery capability;
- supported software and security updates;
- appropriate retention and deletion controls.

Public or unrestricted sharing of Confidential, Highly Confidential or Restricted/Project–Sensitive information shall not be permitted unless expressly authorised and adequately protected.

Cloud administrators shall review privileged access and material security settings periodically and following significant changes or security incidents.

---

10. BIM AND ENGINEERING DATA

EPTM LTD recognises that BIM models, drawings, calculations and engineering documents may constitute highly valuable technical and commercial information.

Appropriate access controls shall therefore be applied to:

- BIM models;
- CAD files;
- engineering calculations;
- technical reports;
- project specifications;
- schedules;
- cost information;
- tender information.

Engineering and project data shall be stored and shared through authorised systems and shall not be disclosed to unauthorised persons.

Project information shall be retained, transferred and disposed of in accordance with applicable contractual, legal, client and Company requirements.

---

11. EMAIL SECURITY

EPTM LTD shall seek to protect email systems against:

- phishing;
- malware;
- credential theft;
- fraudulent payment instructions;
- impersonation;
- malicious attachments;
- malicious links.

Users shall exercise reasonable caution when opening attachments, following links, responding to unusual requests or disclosing information by email.

Unusual financial, payment, credential, technical, project or confidential–information instructions shall be verified through an independent communication channel before action is taken.

Email accounts shall use appropriate authentication and security controls supported by the service.

---

12. PHISHING

Suspected phishing shall be reported promptly through the Company's designated reporting route or to an authorised Company representative.

Users shall not knowingly:

- open suspicious attachments;
- enter credentials into suspicious websites;
- bypass security warnings;
- forward malicious content unnecessarily.

Where a user has entered credentials, opened a malicious attachment, followed a suspicious link or otherwise interacted with suspected malicious content, the matter shall be reported immediately so that containment and investigation can begin without undue delay.

---

13. BACKUPS

EPTM LTD shall maintain or rely upon backup arrangements designed to support recovery from:

- accidental deletion;
- system failure;
- cybersecurity incidents;
- operational disruption.

For systems and information designated as critical or materially important, backup arrangements shall, where technically and commercially practicable:

- use defined backup frequency appropriate to business risk;
- maintain more than one recoverable copy where practicable;
- protect backups against unauthorised access and unauthorised alteration or deletion;
- use logical or physical separation from primary systems where practicable;
- protect sensitive backup data with appropriate access controls and encryption where supported;
- monitor backup completion or failure;
- investigate material backup failures;
- periodically test restoration of selected backups.

Backup frequency and recovery capability shall be proportionate to the importance of the information or system. Critical systems shall have documented recovery priorities and reasonable recovery targets where required by the business or applicable project.

Backups shall not be treated as a substitute for security controls.

---

14. INCIDENT MANAGEMENT

A cybersecurity incident may include:

- unauthorised access;
- malware;
- ransomware;
- phishing;
- credential compromise;
- data loss;
- accidental disclosure;
- system intrusion;
- suspicious activity;
- material service disruption;
- unauthorised alteration or destruction of information.

All suspected incidents shall be reported promptly.

EPTM LTD shall manage material incidents through the following basic operational stages:

1. **Identification and Reporting** – detect, record and escalate the suspected incident;
2. **Assessment and Prioritisation** – determine affected systems, information, users, clients and potential legal or operational impact;
3. **Containment** – take reasonable measures to limit ongoing access, damage, spread or disclosure;
4. **Eradication and Recovery** – remove or mitigate the cause, restore affected services or information from trusted sources where necessary, and verify recovery;
5. **Notification and Communication** – make required internal, client, contractual, regulatory or affected–party notifications;
6. **Post–Incident Review** – record lessons learned and implement reasonable corrective or preventive measures.

The Company Directors or an authorised Company representative shall determine or approve material external communications and notifications unless immediate action is legally required or necessary to prevent further harm.

Incident records shall be maintained for material incidents, including known facts, actions taken, decisions, notifications and corrective measures.

Where legally required, regulatory or affected–party notification shall be undertaken within applicable statutory or regulatory timeframes.

---

15. PERSONAL DATA BREACHES

Where a cybersecurity incident involves personal information, EPTM LTD shall promptly assess whether it constitutes a personal–data breach under applicable law and shall take appropriate action.

Where the UK GDPR notification requirements apply, a notifiable personal–data breach shall be reported to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where required, affected individuals shall also be informed without undue delay.

All personal–data breaches shall be appropriately documented, including where notification is not required.

Applicable client, processor, contractual and jurisdiction–specific notification requirements shall also be considered.

---

16. THIRD PARTIES

Third–party suppliers may be subject to appropriate contractual, security and confidentiality requirements.

Before granting a third party access to sensitive Company or client information or systems, EPTM LTD shall, where proportionate to risk:

- establish the business need and permitted access;
- apply least–privilege access;
- require appropriate confidentiality and security obligations;
- restrict information sharing to what is necessary;
- require notification of material security incidents affecting Company information;
- terminate or review access when the relationship or business need ends.

Third–party security requirements shall be proportionate to the sensitivity of the information and services involved.

---

17. REMOTE WORK

Where remote working is authorised, users shall:

- protect devices;
- use secure connections;
- avoid insecure public systems;
- protect confidential documents;
- prevent unauthorised persons from accessing Company information.

Company information shall not be displayed, discussed, copied or stored where unauthorised persons may reasonably access it.

Remote users shall follow applicable Company authentication, device, cloud, data–handling and incident–reporting requirements.

---

18. PHYSICAL SECURITY

Where applicable, EPTM LTD shall protect:

- devices;
- documents;
- storage media;
- offices;
- confidential information.

Unauthorised persons shall not be permitted access to protected Company systems, devices, documents or information.

Sensitive documents and storage media shall be securely stored, transported and disposed of according to their sensitivity and applicable requirements.

Lost or stolen physical assets containing Company or client information shall be reported promptly.

---

19. SECURITY AWARENESS

EPTM LTD shall maintain reasonable security awareness among personnel concerning:

- phishing;
- social engineering;
- password security;
- information handling;
- data protection;
- device security;
- cyber threats;
- incident reporting.

Personnel shall receive appropriate security information, guidance or training relevant to their responsibilities and level of access.

Security awareness shall be reinforced when material threats, systems, working practices or legal requirements change.

---

20. BUSINESS CONTINUITY

EPTM LTD shall maintain reasonable measures for continuing critical business operations following:

- technical failure;
- cyber incident;
- loss of access;
- communications disruption;
- other significant operational disruption.

For critical business services, continuity arrangements shall, where proportionate to risk:

- identify essential services and information;
- establish recovery priorities;
- identify reasonable alternative working or communication arrangements;
- provide access to essential information through appropriate recovery mechanisms;
- coordinate with relevant suppliers and service providers;
- identify responsible personnel for significant disruption;
- consider dependencies on systems, cloud services, communications and third parties;
- periodically review or test recovery arrangements where practicable.

Recovery shall prioritise protection of people, legal and contractual obligations, critical client commitments, essential business operations and integrity of information.

---

21. INTELLECTUAL PROPERTY

Cybersecurity measures also protect EPTM LTD's and its clients' intellectual property, including:

- designs;
- drawings;
- BIM models;
- reports;
- calculations;
- methodologies;
- specifications;
- presentations;
- commercial materials.

Such information shall be accessed, copied, transmitted, disclosed and stored only for authorised purposes and in accordance with applicable contractual, legal and Company requirements.

---

22. PROHIBITED CONDUCT

Unauthorised activities include:

- accessing systems without authority;
- bypassing security controls;
- installing malicious software;
- stealing credentials;
- deliberately introducing malware;
- unauthorised disclosure of confidential information;
- unlawful interception;

- misuse of Company systems;
- deliberately disabling or materially weakening security controls without authority;
- attempting to obtain, modify, destroy or exfiltrate information without authorisation.

Security testing, vulnerability assessment or penetration testing involving Company systems shall require appropriate Company authorisation before commencement.

---

23. COMPLIANCE

Failure to comply with this Policy may result in:

- access restrictions;
- disciplinary action;
- contractual action;
- termination of access;
- legal action;
- regulatory reporting where required.

EPTM LTD may review compliance with this Policy through reasonable security reviews, access reviews, supplier assessments, incident reviews, audits or other proportionate measures.

Material exceptions to this Policy shall be documented and approved by an authorised Company representative, subject to applicable law and contractual obligations.

This Policy shall be reviewed periodically and when significant changes occur in the Company's operations, systems, threat environment, legal requirements or contractual obligations.

---

24. GLOBAL APPLICATION

This Policy establishes EPTM LTD's global cybersecurity principles and minimum corporate security requirements.

Mandatory local cybersecurity, privacy, data–protection, critical–infrastructure or information–security requirements shall prevail where legally applicable in jurisdictions outside the United Kingdom.

Where client or contractual requirements impose additional lawful security obligations, those requirements shall be addressed as applicable to the relevant engagement or project.

Publication of this Policy does not guarantee that every cybersecurity risk can be eliminated, that every cybersecurity incident can be prevented, or that every law worldwide is automatically satisfied.

EPTM LTD recognises that cybersecurity involves evolving threats, technical limitations, dependencies on third parties and continuously changing legal and operational conditions. Accordingly, the Company shall apply reasonable, proportionate and risk–based measures and shall review and improve its security arrangements as appropriate.