P34B Ltd

Business Policies Document

Cyber Security Policy

Section G

Version P34B-02
July 2025

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.

Contents

Section G: Cyber & Security Policy (2024) 3
G1.0 Introduction 3
G1.1 – Artificial Intelligence Policy 5
Appendix A – Signed Policy and Our Objectives Outlined 9

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.

Section G: Cyber & Security Policy (2024)

G1.0 Introduction

P34B Ltd. recognises the importance of maintaining a strong cybersecurity posture to protect our sensitive information, systems, assets and client confidence. This Cyber & Security Policy outlines the guidelines and procedures that all employees, contractors, and partners must adhere to to ensure the continuing security and privacy of our digital infrastructure and data. The policy applies to all devices, networks, and systems used within the scope of P34B Ltd., including those enhanced by artificial intelligence (AI) technologies. This includes personal mobile devices when in use for work-related purposes.

Compliance with Cyber Essentials Accreditation

P34B Ltd. has achieved Cyber Essentials Accreditation, demonstrating our commitment to implementing fundamental cybersecurity controls. This accreditation is renewed annually. All personnel must comply with the requirements outlined in the Cyber Essentials scheme, as well as any additional security measures mandated by this policy. To assist employees in adhering to the Cyber Essentials Accreditation, a form with guidance on adherence will be sent to employees annually for completion.

Responsibilities

Director:

Neil Horner, as the director of P34B Ltd, holds ultimate responsibility for the overall cybersecurity strategy, implementation, and compliance within the organisation. Neil Horner will review and approve this policy, ensuring its alignment with the business objectives and legal/regulatory requirements. Neil Horner will also collaborate with Clever IT, our current IT partner, to assess and address any emerging cyber threats or vulnerabilities, including those related to AI technologies.

Employees:

All employees are responsible for understanding and complying with this policy. They must exercise caution and good judgment when using company-provided devices, networks, and systems. Employees should report any suspicious activity or security concerns to their immediate supervisor or the designated IT contact.

Information Security

Data Classification and Handling:

All information assets must be classified based on their sensitivity level and handled accordingly. The classification levels include:

- Public: Information that can be freely shared with the public without adverse consequences.
- Internal: Information that should be restricted to authorised personnel within P34B Ltd.
- Confidential: Highly sensitive information that requires strict access controls and protection measures.

Data Protection and Privacy:

P34B Ltd. is committed to protecting the privacy of personal data in accordance with applicable data protection laws. Employees must adhere to the Data Protection Policy and associated procedures when handling personal information.

System Security

Use of Company Devices:

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.

Company-provided devices, such as laptops, mobile phones, and tablets, must only be used for business purposes. Employees should not install unauthorised software or modify system configurations without prior approval from the IT department.

Software Updates and Patches:
All systems and software used within P34B Ltd. must be kept up to date with the latest security patches and updates. Where possible, auto-updates should be enabled. Where this is not possible employees should promptly apply patches and updates provided by the IT department or authorised vendors.

Use of Third-Party Services:
Employees should exercise caution when using third-party services, such as cloud storage or online collaboration tools, to ensure they meet our security requirements. Prior approval must be obtained from the IT department before using such services for business purposes.

AI Integration and Security
AI System Security:
Any AI systems or technologies integrated into P34B Ltd.'s operations must be evaluated for security risks. AI systems should adhere to the same cybersecurity standards and practices as other digital systems within the organisation.

Data Handling in AI Systems:
Data used in AI systems must be classified and handled in accordance with the Data Classification and Handling guidelines. Special attention must be given to ensure that sensitive data is protected when used for training or processing by AI algorithms.

Monitoring AI Systems:
AI systems should be continuously monitored for any anomalies or unusual activities that may indicate a security threat. Regular audits and assessments should be conducted to ensure the AI systems are operating securely and effectively.

Incident Response:
In the event of a cybersecurity incident, all employees must follow the established incident response procedures. This includes promptly reporting any suspected or actual incidents to the IT department. Employees should refrain from discussing or disclosing incident details with unauthorised individuals.

Training and Awareness:
P34B Ltd. will provide cybersecurity training and awareness programs to employees to promote a culture of security. Employees are encouraged to stay informed about the latest cybersecurity threats, trends, and best practices, including those related to AI and where appropriate share them with the P34B Ltd. team.

Review and Compliance:
This policy will be reviewed on an annual basis, or more frequently, if necessary, to ensure its continued effectiveness and alignment with changing security requirements. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

Password and Credential Security
User Passwords:

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.

All users will be issued with (or will be asked to select) a unique individual password which will be changed annually and is confidential to the user. Passwords must adhere to the following guidelines:

- Include three random words, at least one number, and one symbol.
- Capitalise at least one word in the password.
- Passwords must be longer than 12 characters, with no maximum length.

Accessing the P34B network using another employee's username and password without prior authorisation is strictly prohibited and may result in disciplinary action, including summary dismissal.

Compromised or Breached Passwords:
If any passwords are suspected to be compromised or breached, our director will inform all members of the business via phone call or Teams to reset all their passwords.

Password Change Policy
Neil Horner, responsible for Password Management, will ensure all staff are reminded to change passwords annually.

Security Measures to Prevent Brute Force Attacks
To avoid brute force entry to our systems we have the following measures in place:

- Multi-Factor Authentication (MFA)
- Password setup (as per user passwords section above)
- Six-digit PIN numbers
- A code will be required to continue login attempts after four unsuccessful attempts
- Devices will require a restart after five unsuccessful attempts.

Router Access
Access to the routers is forbidden other than with administration access from the directors. Should a member of the team require to reset or access the admin account of the router, the following steps must be followed:
Step 1: Apply via written e-mail to the director requesting access to the router.
Step 2: Notify the reasons for accessing the router.
Step 3: Complete required tasks.
Step 4: Directors to reset the administrative password(s) on the router.

Firewall Passwords and Administration Access
Firewall Password Policy
Our policy will be to change the firewall password annually and whenever a member of the team leaves employment or if it is suspected to be compromised. This will be agreed with our IT partner to ensure compliance.
External Access Through Firewall
On occasions, external parties will require access through our firewall. The process to allow access through our firewalls is strictly at the director level.

- Step 1: Understand the reason for access.
- Step 2: Provide written request to Director(s) for authorisation based on business requirements.
- Step 3: Director provides IP address and any passwords necessary for access.
- Step 4: Passwords are changed, and access is removed

G1.1 – Artificial Intelligence Policy

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.

Introduction

P34B Ltd recognises the growing importance of artificial intelligence (AI) in our operations and services. This AI Policy outlines our commitment to responsible AI use, ensuring it aligns with our values, ethics, and legal obligations. This policy applies to all employees, contractors, and partners using AI within the scope of P34B Ltd.

Ethical Use of AI

P34B Ltd is committed to using AI technologies responsibly and ethically.

We will:

- Ensure AI applications are designed and used to enhance human well-being, respect human rights, and avoid harm.
- Strive for transparency and openness in our AI systems and decision-making processes.
- Avoid the use of AI for illegal, unethical, or discriminatory purposes.
- Regularly assess the societal impact of our AI applications and make improvements as necessary.

Data Privacy and Security

P34B Ltd is dedicated to protecting the privacy and security of data used in AI applications. We will:

- Comply with all applicable data protection laws and regulations.
- Safeguard data against unauthorised access, disclosure, alteration, or destruction.
- Clearly communicate data collection, storage, and usage practices to individuals affected by our AI systems.
- Regularly review and update security measures to mitigate AI-related risks.

Fairness and Bias

P34B Ltd will ensure that our AI systems are designed and tested to be fair and free from bias.

We will:

- Strive for fairness in AI algorithms, avoiding discrimination based on race, gender, age, or other protected characteristics.
- Continuously monitor AI systems for bias and take corrective actions as needed.
- Provide transparency regarding the criteria and data used to train AI systems.

Accountability and Oversight

P34B Ltd acknowledges the need for accountability in AI development and deployment.

We will:

- Assign responsibility for overseeing AI projects, including monitoring compliance with this policy.
- Establish mechanisms for addressing ethical concerns and grievances related to AI use.
- Collaborate with external organisations and experts to ensure ethical AI practices. We will do this through attending local events in Lancashire to keep our knowledge relevant.

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.

Training and Awareness

P34B Ltd will invest in AI training and awareness programs for employees to:

- Enhance understanding of AI principles and best practices.
- Promote responsible AI use within the organisation.
- Keep up-to-date with AI developments and emerging ethical considerations.

Continuous Improvement

P34B Ltd is committed to continuous improvement in our AI practices. We will:

- Regularly review and update this policy to reflect evolving AI technologies and ethical standards.
- Encourage employees and stakeholders to provide feedback and suggestions for AI improvement.
- Conduct regular assessments of AI systems to identify and rectify issues.

Compliance with Laws and Regulations

P34B Ltd will adhere to all applicable laws and regulations governing AI, including but not limited to data protection, intellectual property, and industry-specific regulations.

Conclusion

This AI Policy serves as a foundation for the responsible and ethical use of AI within P34B Ltd. By adhering to these principles and guidelines, we ensure that AI technologies contribute positively to our operations and the broader community.

Confidentiality and Non-Disclosure

P34B Ltd recognises the importance of maintaining the confidentiality of company information and client data when using external AI services or platforms. We are committed to protecting sensitive information and ensuring that it is not disclosed or used inappropriately.

Use of Company Information:

Employees and contractors are prohibited from using company-specific information, including but not limited to client names, proprietary data, trade secrets, and internal processes when using external AI services or platforms. This prohibition extends to any use that could potentially disclose sensitive company information.

Non-Disclosure of Client Data:

When engaging with AI services, employees must ensure that client data and information are not shared or exposed in violation of confidentiality agreements and applicable laws. Any sharing of client data with AI service providers must be done in compliance with client agreements and privacy regulations.

Data Encryption:

When transmitting data to external AI services or platforms, P34B Ltd will use encryption and security measures to protect the confidentiality and integrity of the information being shared.

Vendor Agreements:

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.

P34B Ltd will establish clear agreements with AI service providers that specify the terms of data usage, confidentiality, and non-disclosure to ensure the protection of company and client information.

Employee Training:

All employees and contractors must receive training on the importance of confidentiality and non-disclosure when utilising AI services. They should be aware of the potential risks associated with sharing sensitive information and be diligent in safeguarding it.

Incident Reporting:

In the event of any breach or suspected breach of confidentiality, employees are required to promptly report the incident to the appropriate internal channels for investigation and mitigation.

Contact Information

For questions, concerns, or reporting of AI-related issues, please contact:

Neil Horner at neil.horner@p34b.com.

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.

Appendix G1 – Signed Policy and Our Objectives Outlined

APPENDIX G1
CYBER AND SECURITY POLICY

At P34B Ltd our Cyber and Security policy and our Artificial Intelligence policy is to, so far as is reasonably practicable:

Cybersecurity Objectives:

- *Ensure the security and privacy of sensitive information, systems, and assets.*
- *Comply with Cyber Essentials Accreditation and implement fundamental cybersecurity controls.*
- *Assign responsibilities for cybersecurity at the director and employee levels.*
- *Properly classify and handle information assets based on their sensitivity level.*
- *Implement strong password security and multi-factor authentication (MFA) for all accounts.*
- *At least annually change passwords to meet with our policy requirements.*
- *Protect personal data in accordance with applicable data protection laws.*
- *Maintain up-to-date systems and software with the latest security patches and updates.*
- *Exercise caution when using third-party services and obtain IT partner approval.*
- *Promptly report and respond to cybersecurity incidents following established procedures.*
- *Conduct regular cybersecurity training and awareness programmes for all employees.*

Artificial Intelligence Objectives

- *Use AI technologies responsibly, ethically, and in alignment with human rights and well-being.*
- *Ensure transparency in AI systems and decision-making processes.*
- *Avoid the use of AI for illegal, unethical, or discriminatory purposes.*
- *Protect data privacy and security in all AI applications, complying with relevant laws.*
- *Monitor AI systems for bias, fairness, and unintended consequences.*
- *Assign accountability for AI oversight and compliance with this policy.*
- *Provide training and awareness on AI principles, risks, and best practices.*

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.

- *Prohibit the use of company or client data in external AI platforms without authorisation.*
- *Encrypt and secure data shared with AI service providers.*
- *Establish vendor agreements to ensure confidentiality and responsible data handling.*
- *Continuously review and improve AI practices in line with evolving technologies and standards.*

P34B Ltd will review this policy annually and revise whenever there is a change in circumstances, in work practices or the introduction of new legislation affecting the policy, to ensure that these Cyber & Security and AI standards are maintained.

Signed:

Print Name: P34B Ltd

Date: 08th July 2025

Date for next review: 1st August 2026

P34B Limited - Registered office: 8 Market Place, Adlington, Chorley, Lancashire, England PR7 4EZ
Registered in England and Wales No: 8718019. FSB Membership number 51785622. VAT number: 340668009.