7th September 2026

REFERENCE: P - 013

Wallace Groundwork’s Ltd

Policy

CYBER SECURITY POLICY

Wallace Groundwork's Ltd
The Hub at Gladstone Buildings Broadleys
Chesterfield
Derbyshire
United Kingdom

0. Contents of This Document

1. General Statement of Intent
2. Responsibilities
3. Arrangements
- **3.1.** Cyber Security Risk Assessments
- **3.2.** Security Controls
- **3.3.** Incident Response
- **3.4.** Cyber Security Training
- **3.5.** Supplier & Third Party Management
- **3.6.** Monitoring & Compliance

1. General Statement of Intent

We understand that cyber security is a critical component of our operations and an essential responsibility in today's digital landscape. We are fully committed to safeguarding our valuable assets, including sensitive information, proprietary data, and the systems that support our operations, from cyber threats and vulnerabilities.

Our overarching goal is to establish a robust and resilient cybersecurity posture that aligns with industry best practices and regulatory requirements. We recognise that cyber-attacks are constantly evolving and becoming more sophisticated, and as such, we are dedicated to adopting proactive measures to stay ahead of emerging threats.

Through this comprehensive cyber security policy, we aim to create a culture of security awareness and accountability throughout our organisation. We will promote a strong security mindset among our employees, contractors, and stakeholders, emphasising their role in protecting our information assets and reporting any security concerns promptly.

Key principles of our cyber security policy include:

1. Risk Management: We will conduct regular assessments to identify and assess cyber security risks specific to our organisation. This will enable us to prioritise and implement appropriate controls and mitigation strategies based on the risk level and potential impact.
2. Protection of Information: We will implement robust measures to protect the confidentiality, integrity, and availability of information assets. This includes securing our networks, systems, and data through the use of encryption, access controls, firewalls, intrusion detection systems, and other relevant security technologies.
3. Incident Response and Business Continuity: We will establish an effective incident response plan to address cyber security incidents promptly, minimise their impact, and restore normal operations efficiently. Additionally, we will maintain business continuity plans to ensure our critical operations can continue in the event of a cyber incident.
4. Employee Awareness and Training: We will provide comprehensive cyber security awareness and training programs to all employees, contractors, and relevant stakeholders. This will ensure they are equipped with the necessary knowledge and skills to identify and respond to potential cyber threats, protect sensitive information, and adhere to our security policies and procedures.
5. Compliance and Governance: We are committed to complying with all applicable laws, regulations, and industry standards related to cyber security. We will regularly review and update our cyber security policies and controls to

Wallace Groundwork's Ltd
The Hub at Gladstone Buildings Broadleys
Chesterfield
Derbyshire
United Kingdom

ensure ongoing compliance and effective governance.

6. Continuous Improvement: We recognise that cyber security is an ever-evolving field, and we will continuously monitor, evaluate, and enhance our cyber security measures to adapt to emerging threats and technologies. Regular assessments, audits, and reviews will be conducted to measure the effectiveness of our controls and identify areas for improvement.

By adhering to this cyber security policy, we demonstrate our commitment to protecting our organisation, employees, customers, partners, and stakeholders from the detrimental impacts of cyber threats. We encourage everyone within our organisation to embrace their role in upholding our cyber security principles and report any security concerns promptly.

Author	Nicola Parker
Author Job Role/Position	General Manager
Author Signature	
Signature Date	7th September 2026

Wallace Groundwork's Ltd
The Hub at Gladstone Buildings Broadleys
Chesterfield
Derbyshire
United Kingdom

2. Responsibilities

The functions of the company are designated to the following persons accordingly.

Responsibility	Contact Name	Contact Details
Overall Responsibility for Cyber Security	Peter Wallace	07968357627 p.wallace@wallacegroundworks.com

3. Arrangements

3.1. Cyber Security Risk Assessments

Risk assessment is a crucial component of our cyber security policy, as it helps us identify, evaluate, and prioritise potential risks and vulnerabilities within our organisation's information systems and infrastructure. To ensure effective risk management. We conduct comprehensive and periodic risk assessments to identify potential cybersecurity risks across our systems, networks, and processes. These assessments are carried out by qualified personnel or external experts with expertise in cyber security risk management.

We employ a systematic approach to identify and document potential risks and vulnerabilities. This includes reviewing system configurations, conducting vulnerability scans and penetration tests, analysing threat intelligence, and assessing the impact of potential risks on our organisation's operations and assets.

Identified risks are analysed to assess their likelihood of occurrence and potential impact on our business operations, confidentiality, integrity, and availability of information assets. This evaluation helps us prioritise risks based on their severity and enables us to allocate appropriate resources for risk mitigation.

We establish mechanisms for ongoing monitoring and review of identified risks to ensure their effectiveness and relevance over time. Regular updates to risk assessments are conducted to account for changes in technology, emerging threats, regulatory requirements, and organisational changes.

Risks are treated using a combination of risk mitigation measures, risk transfer, risk avoidance, or acceptance where the residual risk is within acceptable tolerance levels. The decision-making process for risk treatment involves input from relevant stakeholders and considers the cost-effectiveness of proposed mitigation measures.

By implementing robust risk assessment practices, we aim to proactively identify and address potential cyber security risks, minimising the likelihood and impact of security incidents. It is the responsibility of all employees to actively participate in risk assessment activities, report any potential risks they identify, and adhere to the risk mitigation measures outlined in this policy.

3.2. Security Controls

Effective security controls are essential for safeguarding our organization's information assets and protecting against cyber threats. User access rights are granted based on job roles and responsibilities, with regular reviews and updates to ensure access privileges remain appropriate and necessary.

Wallace Groundwork's Ltd
The Hub at Gladstone Buildings Broadleys
Chesterfield
Derbyshire
United Kingdom

We enforce strong authentication measures, such as unique usernames and passwords, to prevent unauthorised access. Passwords are regularly changed, and the use of multifactor authentication (MFA) is encouraged for enhanced security. We implement and maintain secure network architecture, including firewalls, intrusion detection and network segmentation. Regular monitoring and testing are conducted to identify and respond to network security threats promptly.

We utilise encryption techniques to protect sensitive data in transit and at rest. Encryption is applied to data transmitted over public networks, as well as stored on portable devices and in databases, ensuring confidentiality and integrity. We have established an incident response plan that outlines the procedures to be followed in the event of a cyber security incident. This includes incident detection and reporting, containment, eradication, and recovery measures.

3.3. Incident Response

Our Incident Response Plan outlines the steps and procedures to be followed in the event of a cyber security incident within our organisation. The primary objective is to minimize the impact of the incident, restore normal operations, and protect our information assets and systems from further harm.

Any employee who identifies or suspects a cyber security incident must report it immediately to their or any available line manager. The incident and information must then be detailed to the senior IT representative and the senior management team.

Upon receiving a cyber security incident report, the designated IT will initiate an initial assessment to determine the nature and severity of the incident. The response actions may include isolating affected systems or networks, disconnecting from the internet if necessary, and notifying other appropriate stakeholders.

Based on the initial assessment, the incident will be classified according to its severity and impact. The classification will determine the escalation process and the level of response required. Incidents may be classified as low, medium, or high severity, depending on factors such as data sensitivity, system criticality, and potential impact on operations.

For high-severity incidents, an Incident Response Team (IRT) will be activated. The IRT will consist of designated IT and security personnel with specialised knowledge and expertise in handling cyber security incidents. The team will coordinate and execute the response efforts in a timely and effective manner.

The IRT will work to contain the incident and prevent further spread or damage. This may involve isolating affected systems, disabling compromised accounts, restoring from backups, or implementing temporary countermeasures. The objective is to minimize the impact and limit the potential for data loss or unauthorised access.

Once the incident is contained, a thorough investigation and analysis will be conducted to determine the root cause, extent of the impact, and potential vulnerabilities exploited. This may involve forensic analysis, log reviews, system examination, or engagement with external incident response experts, if necessary.

Appropriate stakeholders, including management, legal, and relevant authorities, will be informed of the incident as required by applicable laws and regulations. Communication protocols will be followed to ensure accurate and timely updates to internal and external parties, as well as affected individuals, if applicable.

Once the investigation is completed, the IRT will collaborate with IT and other relevant teams to restore affected systems, validate the security posture, and implement necessary security enhancements to prevent similar incidents in the future.

3.4. Cyber Security Training

Wallace Groundwork's Ltd
The Hub at Gladstone Buildings Broadleys
Chesterfield
Derbyshire
United Kingdom

We recognise that employees play a critical role in ensuring the security of our information assets and the overall cyber resilience of our organisation. To enhance their knowledge and awareness of cyber security best practices, all employees will receive regular training and participate in awareness initiatives.

Our objectives for employee training are to:

- Educate employees on the importance of cyber security and the potential risks associated with cyber threats.
- Provide employees with knowledge and skills to identify and respond to common cyber security threats, such as phishing emails, malware, social engineering, and unauthorised access attempts.
- Promote responsible use of technology resources, including safe browsing practices, secure password management, and data protection.
- Familiarise employees with our organisation's cyber security policies, procedures, and guidelines, ensuring compliance with relevant laws and regulations.
- Empower employees to report any suspicious activities, potential vulnerabilities, or incidents promptly and through the designated reporting channels.

Training sessions will be conducted through various methods to cater to different learning preferences and operational requirements. These methods may include In-person training sessions, online training modules, webinars and virtual workshops and Informational materials.

The training content will cover a range of topics relevant to cyber security, including but not limited to:

- Overview of common cyber threats, their impact, and preventive measures.
- Secure handling of sensitive information, data protection, and privacy considerations.
- Best practices for creating and maintaining strong passwords.
- Safe internet browsing habits, identification of phishing attempts, and email security.
- Responsible use of company devices, networks, and software applications.
- Incident reporting procedures and the importance of timely reporting.
- Compliance with cyber security policies, procedures, and regulatory requirements.

By providing comprehensive training and fostering a culture of cyber security awareness, we aim to empower employees with the knowledge and skills necessary to safeguard our organisation's information assets, protect against cyber threats, and maintain a resilient cyber security posture.

3.5. Supplier & Third Party Management

We recognise that the security of our information assets extends beyond our organisation's boundaries. This arrangement outlines the measures we take to ensure that our suppliers and third-party partners adhere to robust cyber security practices. It aims to minimise potential risks arising from the activities of external entities and maintain the confidentiality, integrity, and availability of our information.

Wallace Groundwork's Ltd
The Hub at Gladstone Buildings Broadleys
Chesterfield
Derbyshire
United Kingdom

Prior to engaging with any supplier or third-party partner, we will conduct a thorough assessment of their cyber security capabilities and practices. This evaluation will consider factors such as their information security policies, incident response procedures, access controls, and data protection measures.

The evaluation will be carried out by designated personnel, in collaboration with relevant stakeholders, such as IT, legal, and procurement departments. We will establish criteria for assessing the cyber security posture of potential suppliers and third-party partners, ensuring alignment with industry best practices, regulatory requirements, and our own cyber security standards.

We will establish ongoing monitoring and assurance of suppliers' and third-party partners' cyber security practices throughout the duration of the engagement including audits, assessments, or security questionnaires which are conducted to evaluate their adherence to contractual obligations and cyber security standards.

In cases where significant cyber security deficiencies are identified, appropriate actions will be taken, which may include remediation plans, termination of the engagement, or additional security controls.

Suppliers and third-party partners will be required to promptly report any cyber security incidents or breaches that impact our organisation's information assets or systems.

3.6. Monitoring & Compliance

We will regularly review and update our cyber security policies, procedures, and controls to align with industry best practices and regulatory requirements. This ensures that our practices remain relevant and effective in addressing evolving cyber threats and changing business needs. We will actively engage with the wider cyber security community, industry forums, and information-sharing platforms to stay informed about emerging threats, vulnerabilities, and best practices. This collaboration will enable us to leverage collective knowledge and expertise to enhance our security posture.

We will monitor our compliance with internal policies, industry standards, and applicable regulatory requirements related to cyber security. Regular compliance assessments and audits will be conducted to identify any gaps or non-compliance issues and initiate corrective actions.

Wallace Groundwork's Ltd
The Hub at Gladstone Buildings Broadleys
Chesterfield
Derbyshire
United Kingdom

I have read and understood the entirety of this document. Where there was something I did not fully understand, it was explained to my satisfaction. I agree to comply with the required directions and instructions in this document. If at any point, I cannot comply, I will highlight this before continuing.			
Name	**Job Role / Position**	**Signature**	**Date**

Wallace Groundwork's Ltd
The Hub at Gladstone Buildings Broadleys
Chesterfield
Derbyshire
United Kingdom

I have read and understood the entirety of this document. Where there was something I did not fully understand, it was explained to my satisfaction. I agree to comply with the required directions andinstructions in this document. If at any point, I cannot comply, I will highlight this before continuing.			
Name	**Job Role / Position**	**Signature**	**Date**

Email: n.parker@wallacegroundworks.com
Website: www.wallacegroundworks.com
Phone: 01246957197