



INFORMATION SECURITY POLICY

HEX 101 LTD

Version 3.0 | Effective from 1 September 2026

Document Owner	HEX 101 LTD – Management / Information Security Lead
Approved By	Director / Authorised Management Representative
Effective Date	1 September 2026
Version	3.0
Review Frequency	At least annually, and after material changes or significant security incidents
Classification	Internal – Controlled Document

Applies to HEX 101 personnel, contractors and authorised third parties, and to Company and customer systems, information and services accessed or managed by HEX 101.

1. Purpose

This Information Security Policy establishes the principles, responsibilities and minimum security controls HEX 101 LTD (HEX 101) applies to protect its own information, systems, services and assets, and to protect customer information and customer environments where HEX 101 is authorised to access or manage them.

As a managed service provider (MSP), HEX 101 may hold privileged access to customer systems, networks, endpoints, cloud platforms, identities, backups and business applications. This creates additional security responsibilities. HEX 101 therefore applies a risk-based approach designed to protect confidentiality, integrity and availability.

This policy supports good practice and applicable legal, contractual and regulatory requirements. It is not a claim that HEX 101 holds any particular certification or accreditation.

2. Scope

- All employees, directors, contractors, temporary workers and other personnel with access to Company or customer information.
- Company-owned, leased or managed devices, servers, networks, cloud services, applications, storage, communications systems and security tools.
- Customer systems and environments that HEX 101 accesses, supports, monitors, administers or manages under an agreed service.
- Information in electronic, physical, verbal or other forms.
- Remote, home and mobile working.
- Third parties, suppliers, subcontractors and technology partners with relevant access.

3. Information Security Objectives

- Confidentiality – information is accessible only to authorised people and systems.
- Integrity – information and systems are protected against unauthorised alteration, corruption or destruction.
- Availability – critical systems and information remain available and can be restored.
- Accountability – security-relevant activity is attributable to an individual, service account or authorised system where practicable.
- Resilience – appropriate preventative, detective, response and recovery controls are maintained.
- Compliance – controls reflect applicable law, contracts, customer requirements and risk.

4. Governance and Responsibilities

4.1 Management

- Ensure information security has appropriate authority, resources and oversight.
- Review significant security risks, incidents, exceptions and improvement actions.
- Ensure material security obligations are reflected in contracts and service arrangements.

4.2 Information Security Lead / Responsible Person

- Maintain this policy and coordinate the information security framework.
- Coordinate risk assessments, security reviews, incident management and improvement actions.
- Oversee security registers, including assets, risks, incidents and suppliers as appropriate.
- Coordinate security awareness and escalate material risks.

4.3 All Personnel

- Comply with this policy and related procedures.
- Protect credentials, devices, information and customer access.
- Use systems only for authorised purposes.
- Report suspected incidents, phishing, lost devices and accidental disclosure promptly.
- Complete required security training.

5. Risk Management

HEX 101 will identify, assess and manage information security risks using a proportionate, risk-based approach. Assessments should consider the information, systems, services, customer impact, likelihood and potential consequences.

- Material risks should be recorded with an owner and treatment action.
- High or unacceptable risks should be escalated to management.
- Risks should be reviewed after significant technology, service, customer, supplier or threat changes.
- Customer-specific security requirements should be recorded and incorporated into applicable service arrangements.

6. Asset Management and Information Classification

6.1 Asset Management

- Company endpoints, servers, networking equipment, mobile devices and security appliances should be identifiable and assigned to an owner.
- Software and cloud services should be approved before being used to store or process Company or customer information.
- Unsupported or obsolete software should be removed, upgraded or subject to documented risk treatment.

- Assets leaving Company control must be returned, securely wiped, destroyed or appropriately disposed of.

6.2 Information Classification

- Public – intentionally approved for public release.
- Internal – routine Company information not intended for public release.
- Confidential – commercially sensitive, customer, contractual, operational or personal information requiring controlled access.
- Restricted – highly sensitive information, including privileged credentials, security configurations, authentication secrets and information whose compromise could cause significant harm.

7. Access Control and Identity Management

Access to Company and customer systems will be authorised, controlled and reviewed according to business need and risk. Least privilege is a core requirement for MSP operations.

- Use unique individual accounts wherever practicable; avoid shared accounts.
- Enable MFA for administrative, remote and cloud access wherever supported and appropriate.
- Separate privileged access from ordinary user activity where practical.
- Grant administrative access only to authorised personnel and only for the required scope.
- Remove or amend access promptly when personnel leave, change role or no longer require access.
- Review privileged and other higher-risk access periodically.

-
-
- Control break-glass/emergency accounts and monitor their use. Define ownership and secure credentials for service accounts.
- Do not store credentials, API keys, certificates or tokens in plain text.
- Change default passwords before operational use.
- Do not reuse customer credentials between customers or unrelated environments.

8. Authentication and Password Security

- Use strong, unique passwords/passphrases where passwords are required.
- Use MFA for privileged, remote, cloud and other higher-risk access where supported.
- Never disclose authentication secrets to unauthorised persons.
- Use an approved password manager for business credentials where available.
- Change or revoke credentials suspected of compromise.
- Use strong or phishing-resistant MFA mechanisms for privileged access where practical.

9. Endpoint, Server and Network Security

- Use supported operating systems and applications where reasonably practicable.
- Apply security updates and patches according to risk, vendor guidance and customer requirements.
- Deploy appropriate endpoint protection/EDR and host firewall controls.
- Disable unnecessary services, ports, protocols and accounts where practical.
- Use device encryption where supported and appropriate.
- Do not expose administrative interfaces directly to the public internet unless required and appropriately controlled.
- Use segmentation, VPN, firewalling and conditional access according to risk and service design.
- Protect and back up important network/security configurations where appropriate.

10. Remote Access and MSP Privileged Access

- Use Company-approved or customer-approved secure remote administration mechanisms.
- Restrict RMM/remote-access tools to authorised personnel and protect them with MFA where supported.
- Make remote access attributable to an individual wherever technically practicable.
- Access customer environments only for legitimate service, support, maintenance or incident purposes.
- Do not use customer administrative access for personal or unrelated activity.
- Log or otherwise attribute remote sessions where the technology permits.
- Remove temporary/elevated access when no longer required.
- Review and remove unused remote-access tools.
- Cooperate with customer requirements concerning approval, monitoring and notification of privileged access.

11. Vulnerability and Patch Management

HEX 101 will maintain a risk-based process for identifying, prioritising and remediating vulnerabilities in systems it manages.

- Use vendor advisories, security tooling, scanning, monitoring, testing and incident findings to identify vulnerabilities.
- Prioritise critical and actively exploited vulnerabilities for urgent assessment.

-
-
- Use compensating controls and documented risk decisions where remediation is not immediately possible. Identify and manage end-of-life software and systems.
- Monitor patch status for managed systems where patching is within service scope.
- Respect customer maintenance windows and change-control requirements.

12. Change and Configuration Management

- Authorise, document and test material changes as appropriate.
- Consider security impact, availability and rollback requirements.
- Document emergency security changes retrospectively as soon as practical.
- Use approved secure configuration baselines where practical.
- Apply additional scrutiny to changes involving firewalls, privileged access, identity, backups and security tools.

13. Data Protection and Privacy

Where HEX 101 processes personal data, it will apply appropriate technical and organisational measures proportionate to risk. This includes confidentiality, integrity and availability, access control, resilience, restoration, testing and risk assessment.

- Access personal data only for legitimate and authorised purposes.
- Do not copy, export or retain personal data unnecessarily.
- Encrypt personal data in transit and at rest where appropriate to risk and technical environment.
- Report suspected personal data breaches under the Company's incident and breach procedures.
- Where HEX 101 acts as a processor, process data in accordance with the customer contract and documented instructions.
- Use only authorised and appropriately contracted sub-processors.
- Follow applicable retention and deletion requirements.
- Do not use customer data for unrelated purposes unless authorised and lawful.

Processor contracts should address permitted processing, confidentiality, security measures, breach notification, sub-processing and return/deletion requirements as appropriate.

14. Encryption and Key Management

- Use encryption where appropriate to protect confidential and restricted information.
- Use full-disk/device encryption on portable devices where technically available and appropriate.
- Use secure protocols such as TLS/HTTPS, SSH and approved VPN technologies.
- Protect encryption keys, certificates and secrets from unauthorised access.
- Rotate, renew or revoke keys and certificates according to risk and service requirements.
- Do not treat encryption as a substitute for access control, monitoring or secure configuration.

15. Email, Collaboration and Communications Security

- Use approved business email and collaboration platforms.
- Enable MFA and appropriate identity protections for business email/cloud services.
- Remain alert to phishing, business email compromise, malicious links, attachments and impersonation.

-
-
- Do not send sensitive information to unintended recipients.
- Restrict external sharing to intended recipients and expire links where appropriate.
Use SPF, DKIM and DMARC appropriately for Company domains where supported. Report suspicious messages promptly.

16. Backup, Business Continuity and Disaster Recovery

HEX 101 will maintain backup and recovery arrangements appropriate to the importance of its services and the services it is contracted to manage. Critical data should be backed up and restoration tested periodically.

- Back up critical Company data and configurations according to recovery requirements.
- Configure customer backups in accordance with the service agreement and customer requirements.
- Protect backups from unauthorised access and, where appropriate, from the same compromise affecting production systems.
- Protect backup credentials using strong access controls and MFA where supported.
- Perform restoration tests for critical services or where contractually required.
- Document RTO/RPO requirements where applicable.
- Consider loss of premises, personnel, connectivity, cloud services, cyber attack and supplier failure.
- Record and correct material recovery failures.

17. Security Monitoring, Logging and Detection

- Log security-relevant events where feasible and proportionate.
- Logs may include authentication, privileged access, administrative actions, security alerts, endpoint, firewall, backup and configuration events.
- Protect logs from unauthorised alteration and access.
- Monitor proportionately to service scope and contractual requirements.
- Investigate security alerts according to severity.
- Use logs to support incident response and customer reporting where appropriate.

18. Incident Management and Breach Response

HEX 101 will maintain an incident response process for suspected or confirmed information security incidents.

1. Identify and report the incident.
2. Assess severity, affected systems, customers, information and impact.
3. Contain the incident.
4. Escalate to management and relevant customer contacts.
5. Investigate and preserve appropriate evidence.
6. Eradicate the cause and restore systems through controlled recovery.
7. Assess regulatory, contractual and data-protection notification requirements.
8. Record the incident and lessons learned.
9. Implement corrective and preventative actions.

Personnel must not make external statements about security incidents on behalf of HEX 101 unless authorised. Customer communications will follow the applicable contract and escalation plan.

-
-

19. Security Awareness and Personnel Security

- Provide appropriate security awareness training.

- Cover phishing, passwords/MFA, data handling, social engineering, acceptable use, incident reporting and remote working.
- Provide role-specific security training to privileged technical personnel.
- Include security responsibilities in onboarding and offboarding.
- Maintain confidentiality obligations after employment/engagement ends.
- Remove access promptly when employment or engagement ends.

20. Acceptable Use

- Use Company systems and customer environments only for authorised purposes.
- Do not install unauthorised software or remote-access tools.
- Do not access systems or data beyond authorised permissions.
- Do not use Company resources for unlawful activity or to introduce malicious code.
- Do not disable or circumvent security controls without authorisation.
- Use removable media cautiously and encrypt sensitive information where appropriate.

21. Physical and Environmental Security

- Restrict access to Company premises, offices, server areas and equipment according to risk.
- Control visitors and escort them where required.
- Protect laptops/mobile devices from theft or unauthorised viewing.
- Securely store and destroy sensitive paper records.
- Protect equipment from relevant fire, water, temperature and power risks.
- Handle customer equipment removed for repair/decommissioning/disposal according to chain-of-custody requirements.

22. Secure Disposal and Data Sanitisation

- Securely sanitise or physically destroy storage media before disposal, reuse or transfer where required.
- Use a sanitisation method appropriate to the media, technology and risk.
- Document custody, asset identification and sanitisation/destruction for relevant decommissioning services.
- Issue destruction certificates or equivalent evidence where required by the service or contract.
- Use appropriately authorised disposal/recycling providers and follow applicable environmental requirements.

23. Supplier and Third-Party Security

- Assess security risks associated with suppliers, cloud providers, subcontractors and technology partners according to risk.
- Include appropriate confidentiality, security, data protection, incident and access provisions in contracts where relevant.
- Authorise third parties before granting access.
- Apply least privilege and remove third-party access when no longer required.
- Obtain required customer authorisation and contractual safeguards for sub-processors.
- Review critical suppliers proportionately, including resilience and security.

24. Customer Environment Security

MSP security responsibilities may be shared between HEX 101 and its customers. The applicable contract, service description or other written agreement should identify material responsibilities.

- Apply agreed controls to systems within HEX 101's management scope.
- Customers remain responsible for systems, data, accounts and controls expressly outside HEX 101's scope.
- Follow lawful and authorised customer instructions.
- Notify customers through agreed channels where a material security weakness outside HEX 101's direct control is identified.
- Apply customer-specific security standards where agreed in writing.
- Escalate requests to weaken security controls where doing so would create unacceptable risk.

25. Security Testing and Assurance

- Review security controls periodically.
- Use vulnerability scanning, configuration reviews, penetration testing, phishing simulations, restore testing or other assurance activities where proportionate.
- Authorise and scope testing carefully, especially in customer environments.
- Risk-rate findings and assign remediation or authorised risk acceptance.
- Retain appropriate evidence of important tests and reviews.

26. Records, Evidence and Audit

- Retain appropriate evidence that key security controls are implemented, reviewed or tested.
- Records may include access reviews, training, incidents, risk assessments, backup tests, vulnerability reports, changes and supplier assessments.
- Protect records from unauthorised alteration and retain them appropriately.
- Handle customer audits and assurance requests according to contractual terms and reasonable security constraints.

27. Exceptions and Risk Acceptance

Security exceptions must be documented rather than handled informally.

- Record the affected system/service, reason, risk and duration.
- Consider compensating controls.
- Obtain appropriate management approval and, where relevant, customer approval.
- Assign an owner and review/expiry date.
- Review material exceptions during security and management reviews.

28. Compliance and Legal Requirements

HEX 101 will comply with applicable laws and contractual requirements relevant to its activities, including where applicable UK data protection requirements, confidentiality obligations, contractual security requirements, employment obligations and requirements relating to technology and equipment disposal.

Security controls will be risk-based and proportionate to the nature, scope, context and purpose of processing and the risks involved.

29. Policy Review and Continuous Improvement

- Review this policy at least annually.
- Review after significant incidents, major technology/service changes, changes in law/regulation or material changes in risk.
- Use lessons from incidents, audits, testing and customer feedback to improve controls.
- Require authorised management approval for policy changes.

30. Related Policies and Procedures

This policy is the overarching information security policy and should be supported by detailed procedures and standards as appropriate, including:

- Access Control and Privileged Access Procedure
- Acceptable Use Policy
- Password and Authentication Standard
- Data Protection and Data Breach Procedure
- Incident Response Procedure
- Backup and Disaster Recovery Procedure
- Business Continuity Plan
- Vulnerability and Patch Management Procedure
- Change Management Procedure
- Asset Management and Secure Disposal Procedure
- Supplier / Third-Party Security Procedure
- Joiner, Mover and Leaver Procedure
- Remote Working and Mobile Device Policy
- Security Awareness and Training Procedure
- Risk Management Procedure

31. Minimum Security Baseline for HEX 101 Managed Services

Unless a customer service agreement specifies otherwise, the following controls represent HEX 101's intended baseline, subject to technical feasibility, customer approval and risk.

Control Area	Minimum Baseline
Identity	MFA for privileged/cloud/remote access where supported; unique accounts; least privilege.
Endpoint	Supported operating systems; security updates; endpoint protection; encryption where appropriate.
Remote Management	Approved RMM tools; restricted admin access; MFA where supported; logging/attribution where available.
Network	Firewalling; secure administration; controlled inbound access; segmentation where appropriate.
Email	MFA; anti-phishing controls; appropriate email security configuration; user awareness.
Backups	Backups appropriate to service requirements; protected credentials; periodic restoration checks for critical services.
Monitoring	Security alerts and relevant logs monitored according to service scope.
Vulnerability	Risk-based vulnerability identification, prioritisation and remediation.

Incident Response	Documented escalation and response; customer notification according to contract.
Data Protection	Appropriate technical/organisational measures; controlled access; secure transfer and disposal.
Supplier Security	Authorised suppliers; proportionate due diligence; contractual security/data protection requirements.
Offboarding	Prompt removal of access; return/deletion/sanitisation of Company and customer assets as applicable.

32. Approval

This policy is approved for use by HEX 101 LTD from the effective date stated on the front page.

Approved by	_____ Ms Lorna Bucknall
Position	Director / Signed by: Authorised Management Representative
Signature	_____ <i>Lorna Bucknall</i>
Date	__ 1 st September 2026 FA743F...