Maclean Of Duart Enterprises

Privacy Policy & Information Security / Data Handling Policy

Effective Date: September 25, 2026
Combined Policy Document

This document combines the company's public-facing Privacy Policy with its internal Information Security & Data Handling Policy.

Privacy Policy

Effective Date: September 25, 2026

Purpose

Maclean Of Duart Enterprises is committed to protecting the privacy, confidentiality, integrity, and security of information entrusted to us. We follow a privacy-by-design and security-by-default approach and seek to collect, access, retain, and disclose only information reasonably necessary to provide our services, operate our business, meet contractual obligations, protect our clients, and comply with applicable law.

Information We May Collect

- Name, business name, address, telephone number, and email address.
- Service, billing, scheduling, and transaction information.
- Device, network, system, diagnostic, security, and technical information.
- Information voluntarily provided by a client.
- Client data temporarily accessible while performing IT support, cybersecurity, repair, backup, recovery, administration, or related services.
- Website information reasonably necessary for security, operation, diagnostics, and communications.
- We do not intentionally collect information that is unnecessary for the service being provided.

Client Systems and Data

Access to a client's computer, network, account, files, credentials, or other information is limited to what is reasonably necessary and authorized for the requested work. Information encountered while providing technical services remains confidential. We do not inspect, copy, retain, disclose, or use client content except as reasonably necessary to perform authorized services, protect systems, comply with contractual obligations, or comply with applicable law. Client information is not sold or rented.

Security

We use administrative, technical, and physical safeguards appropriate to the nature and sensitivity of information under our control. Where appropriate, these safeguards may include encryption, multi-factor authentication, access controls, secure credential management, system hardening, logging, backups, malware protection, vulnerability management, secure communications, and restricted access based upon legitimate business need. Our security practices are informed by recognized cybersecurity principles and frameworks, including the NIST Cybersecurity Framework. No information system can be guaranteed to be completely secure; we therefore seek to reduce foreseeable risks rather than represent that any system is immune from compromise.

Passwords and Credentials

Clients should not provide passwords or authentication credentials unless reasonably necessary for authorized services. Credentials entrusted to us are restricted to authorized use. We seek to avoid unnecessary storage of passwords and other authentication secrets and use appropriate safeguards when credentials must be temporarily stored or transmitted. We will never sell client credentials or use them for purposes unrelated to authorized services.

Data Minimization and Retention

We retain personal and client information only for as long as reasonably necessary for the purpose for which it was collected, legitimate business requirements, contractual obligations, security requirements, dispute resolution, or applicable law. Information that is no longer reasonably required will be securely deleted, destroyed, anonymized, or otherwise rendered inaccessible when reasonably practicable.

Third-Party Services

We may use reputable service providers when reasonably necessary to operate our business or provide requested services. We seek to limit information provided to third parties to what is necessary for their function and to select providers with appropriate privacy and security safeguards. We do not authorize service providers to sell client information provided to them by us.

Disclosure of Information

- Authorized or requested by the client;
- Necessary to provide an authorized service;
- Necessary to investigate or respond to a security incident;
- Necessary to protect our clients, systems, property, or legal rights; or
- Required by applicable law, court order, subpoena, or other lawful governmental process.
- Where legally permitted and reasonably practicable, we seek to limit disclosures to the information necessary for the applicable purpose.

Security Incidents and Data Breaches

Suspected security incidents involving information under our control will be investigated promptly. When applicable law requires notification following a breach of personal information, we will provide required notifications to affected persons, clients, governmental authorities, or other required parties in accordance with applicable federal and Pennsylvania law. We maintain incident-response practices intended to contain incidents, preserve relevant evidence, determine their scope, mitigate harm, restore affected systems, and reduce the likelihood of recurrence.

Client Privacy Rights

Clients may contact us to request information about personal information maintained by us or to request correction or deletion of information. Requests will be honored where reasonably practicable and consistent with applicable contractual, security, recordkeeping, and legal obligations.

Children's Information

Our services are not directed toward collecting personal information from children. We do not knowingly collect children's personal information through our website except where necessary for an authorized service and appropriately permitted by law.

Changes to This Policy

This Privacy Policy may be revised as our services, security practices, technologies, or legal obligations change. The current version will supersede previous versions upon publication unless otherwise stated.

Contact

Maclean Of Duart Enterprises
Email: office@macleanofduartenterprises.com
Phone: 717-500-6202
Website: macleanofduartenterprises.com

Information Security & Data Handling Policy

Effective Date: September 25, 2026 | **Review Cycle:** At least annually and after significant changes

1. Purpose

Maclean Of Duart Enterprises maintains this policy to protect company, client, employee, contractor, and third-party information against unauthorized access, disclosure, alteration, destruction, loss, misuse, or disruption. Security shall be implemented according to least privilege, zero trust, defense in depth, data minimization, secure-by-default configuration, need-to-know access, and continuous risk management.

2. Scope

- All employees, owners, contractors, and authorized personnel;
- Computers, servers, mobile devices, networks, applications, and cloud systems;
- Client devices and systems accessed during service;
- Company and client credentials;
- Electronic and physical records, backups, and removable media;
- Remote-support systems and third-party services processing company or client information.

3. Security Framework

The Company's cybersecurity program shall be informed, where applicable, by the NIST Cybersecurity Framework, CIS Critical Security Controls, CISA cybersecurity guidance, applicable federal and Pennsylvania law, contractual security requirements, and industry-specific requirements. These frameworks guide security practices but do not constitute a representation of formal certification unless certification has actually been obtained.

4. Data Classification

Information shall be classified as Public, Internal, Confidential, or Restricted/Sensitive. Restricted/Sensitive information includes passwords, authentication secrets, encryption keys, personally identifiable information, financial information, security configurations, recovery codes, private keys, and protected client information. The highest applicable classification governs combined information.

5. Data Minimization

Only information reasonably necessary to perform authorized business or technical functions shall be collected or accessed. Client files shall not be browsed, copied, analyzed, retained, or transferred merely because technical access makes them available.

6. Access Control

Access shall follow least privilege and need-to-know principles. Personnel shall receive only the minimum permissions necessary. Administrative accounts shall be separated from ordinary user accounts where reasonably practicable. Shared administrative credentials should be avoided. Access shall be revoked promptly when no longer required.

7. Authentication

Multi-factor authentication shall be required wherever reasonably available for administrative accounts, remote access, cloud administration, email, password managers, source-code repositories, financial systems, backup administration, domain/DNS administration, and systems containing sensitive client information. Phishing-resistant authentication such as passkeys or hardware security keys should be preferred for high-risk accounts.

8. Credential Management

Passwords, API keys, private keys, recovery codes, authentication tokens, and similar secrets shall be treated as Restricted information. Credentials shall not be stored in plaintext documents, ordinary notes, email, source code, or other insecure locations. Reputable encrypted password or secrets management shall be used where retention is necessary.

9. Encryption

Sensitive information shall be encrypted in transit using current secure protocols wherever reasonably practicable. Sensitive information on company-controlled portable devices and backups shall receive appropriate encryption. Obsolete or insecure cryptographic protocols and algorithms shall not knowingly be used when secure alternatives are reasonably available.

10. Client Devices and Systems

- Access only systems necessary for authorized work;
- Avoid accessing unrelated personal files;
- Avoid unnecessary copying of client information;
- Obtain authorization before material system changes;
- Protect devices while in Company custody;
- Remove temporary working copies when no longer necessary;
- Close or terminate remote-access sessions when work is completed.

11. Remote Support

Remote access shall require explicit client authorization or an established service agreement authorizing such access. Remote-support systems shall use encrypted communications and appropriate authentication. Unattended remote access shall not be installed or enabled without authorization. Persistent administrative access shall be limited and periodically reviewed.

12. Endpoint and Network Security

Company systems shall use appropriate controls including supported software, patch management, firewalls, malware protection, secure configuration baselines, device encryption, automatic screen locking, restricted administrative privileges, secure networking practices, and logging/monitoring. Unsupported systems shall be isolated, upgraded, replaced, or otherwise risk-managed where reasonably practicable.

13. Vulnerability and Patch Management

Known vulnerabilities shall be evaluated according to severity, exploitability, exposure, and operational risk. Critical actively exploited vulnerabilities shall receive priority remediation. Where immediate patching is impossible, compensating controls shall be considered.

14. Software and Open-Source Security

Software shall be obtained from trusted sources whenever reasonably practicable. Applications and dependencies shall be maintained and reviewed for known vulnerabilities appropriate to their risk. Open-source software may be used where appropriate and evaluated for security, maintenance status, provenance, licensing, community support, and suitability.

15. Logging and Monitoring

Security-relevant systems should maintain appropriate audit logs, which may include authentication attempts, administrative actions, security alerts, remote-access activity, system changes, and backup activity. Logs containing sensitive information shall themselves be protected, and logging shall not intentionally collect unnecessary private client content.

16. Backups

Critical company information shall be backed up according to operational importance. Where appropriate, backup architecture should include multiple copies and separation from production systems, with at least one backup protected against ordinary modification or deletion. Restoration procedures shall be periodically tested where appropriate.

17. Removable Media

Unknown or untrusted removable media shall not be connected to company or client systems. Sensitive information stored on removable media shall be encrypted where appropriate. Media shall be securely erased or physically destroyed before disposal when it contains sensitive information.

18. Data Retention and Secure Destruction

Information shall be retained only as long as reasonably necessary for services, operations, security, contractual obligations, accounting, dispute resolution, or applicable legal requirements. Information no longer required shall be securely deleted, cryptographically erased, destroyed, anonymized, or otherwise rendered inaccessible as appropriate.

19. Email and Electronic Communications

Sensitive information should not be transmitted through insecure communications when a reasonably secure alternative is available. Personnel shall exercise caution regarding phishing, impersonation, unexpected attachments, links, payment requests, password requests, and changes to financial instructions. High-risk instructions should be independently verified through a trusted channel.

20. Third-Party and Supply-Chain Security

Third-party services shall be selected with consideration for security and privacy. Vendor access shall be limited to what is reasonably necessary. Where appropriate, vendors handling sensitive information should provide suitable security, confidentiality, incident-reporting, retention, and deletion protections.

21. Incident Response

Suspected cybersecurity incidents shall be investigated promptly. Response shall generally include identification, triage/classification, containment, preservation of relevant evidence, eradication, recovery, required communications/notifications, and post-incident review. Personnel shall not conceal known security incidents.

22. Data Breach Response

A suspected compromise of personal, confidential, or restricted information shall be escalated promptly. The Company shall determine affected information and persons, unauthorized acquisition/access, credential revocation needs, containment requirements, forensic needs, contractual obligations, and applicable breach-notification requirements.

23. Business Continuity and Recovery

The Company shall maintain reasonable procedures for restoring critical operations following ransomware, hardware failure, data loss, natural disaster, provider failure, or other significant disruption. Recovery priorities are: People -> Communications -> Security -> Critical Data -> Critical Systems -> Normal Operations.

24. Physical Security

Devices and records containing sensitive information shall be reasonably protected against theft, unauthorized access, loss, and environmental damage. Portable devices shall not be left unsecured where unauthorized persons could readily access them.

25. Mobile Devices

Mobile devices accessing sensitive company or client information shall use appropriate screen locking, encryption where supported, current security updates, strong authentication, lost-device protections where appropriate, and restrictions on untrusted software. Lost or stolen devices containing company or client information shall be reported immediately.

26. Security Awareness

Personnel with access to company or client systems shall receive security guidance appropriate to their responsibilities, including phishing, social engineering, credential theft, malware, unauthorized disclosure, physical security, remote access, and incident reporting.

27. Artificial Intelligence and External Processing

Confidential, Restricted, client-controlled, credential, proprietary, or personally identifiable information shall not be submitted to public artificial-intelligence systems or other external processing services unless authorized and appropriate safeguards are in place. AI tools shall not be presumed confidential merely because access requires an account.

28. Client Separation

Information belonging to one client shall not be intentionally disclosed to another. Where multiple clients are administered using common infrastructure, appropriate logical separation and access controls shall be maintained. Credentials should be unique between clients wherever technically feasible.

29. Security Testing

Security testing, vulnerability scanning, penetration testing, password testing, network discovery, or similar activity shall be performed against client systems only with appropriate authorization. Potentially destructive testing shall require additional consideration and authorization.

30. Exceptions

Exceptions shall be based on legitimate operational requirements, documented where appropriate, limited in scope and duration, and accompanied by reasonable compensating controls when feasible. Convenience alone is not sufficient justification for materially weakening protection of Restricted information.

31. Enforcement

Failure to comply may result in suspension or revocation of system access, disciplinary action, termination of contractual relationships, or other appropriate corrective action. Suspected violations shall be investigated proportionately to severity.

32. Continuous Improvement

Maclean Of Duart Enterprises shall periodically evaluate its security controls, threats, vulnerabilities, technology, legal requirements, and business operations and modify security practices when reasonably necessary. Material incidents and identified weaknesses shall be used to improve safeguards.

33. Policy Review

This policy shall be reviewed at least annually and following significant cybersecurity incidents, changes in applicable law, business operations, technology or infrastructure, threat conditions, or recognized cybersecurity standards.

Maclean Of Duart Enterprises
Phone: 717-500-6202
Email: office@macleanofduartenterprises.com
Website: macleanofduartenterprises.com

Document Classification: Internal / Controlled Distribution (Information Security & Data Handling Policy)

Implementation note: This document establishes company policy and operational expectations. Applicable laws, contracts, client requirements, and regulatory obligations control where they impose additional or conflicting requirements.