Data Security & Privacy Policy

Policy Number: SEC-2024-001 | **Last Updated:** March 2024
Applies to: All ClearPath Employees, Contractors, and Third-Party Partners

Purpose and Scope

This Data Security and Privacy Policy establishes requirements for protecting ClearPath and customer data. All employees, contractors, and third-party partners with access to ClearPath systems must comply with this policy. Violations may result in disciplinary action up to and including termination and legal action.

ClearPath is committed to maintaining the confidentiality, integrity, and availability of all information assets. We comply with GDPR, CCPA, SOC 2 Type II, and other applicable data protection regulations.

1. Data Classification

ClearPath classifies all data into three categories based on sensitivity. Appropriate handling procedures must be followed for each classification level:

Classification	Definition	Examples	Handling Requirements
Public	Information intended for public consumption	Marketing materials, blog posts, published documentation, press releases	No special handling required. Can be shared freely
Internal	Information for internal use only	Business plans, internal memos, employee directory, meeting notes, roadmaps	Share only with ClearPath employees. Do not post publicl
Confidential	Highly sensitive information requiring protection	Customer data, PII, source code, financial records, security credentials, API keys	Encrypt at rest and in transit. Access requires approval. M

2. Access Control

Password Requirements: All work accounts must use strong passwords meeting these minimum requirements:
- Minimum 12 characters in length
- Include uppercase letters, lowercase letters, numbers, and symbols
- Cannot be a previously used password
- Cannot contain common dictionary words or personal information
- Must be changed every 90 days for accounts accessing confidential data
- Never share passwords or write them down

Multi-Factor Authentication (MFA): MFA is required for:
- All email accounts (Google Workspace)
- GitHub and code repositories
- AWS and cloud infrastructure
- Admin panels and production systems
- VPN access
- Any system containing confidential data

Use Google Authenticator, 1Password, or hardware security keys (YubiKey). SMS-based MFA is not permitted for production systems due to security risks.

Access Provisioning: Access to systems and data follows the principle of least privilege:
- New employees receive baseline access on day 1 (email, Slack, HR systems)
- Additional access requires manager approval via the IT ticketing system
- Access to confidential data requires documented business need and security training
- Access is reviewed quarterly; unused access is automatically revoked
- Upon termination, all access is revoked within 1 hour

3. Data Handling and Storage

Approved Tools and Services: Use only company-approved tools for storing and sharing data:

Purpose	Approved Tools	Prohibited
Documents & Files	Google Drive, Notion	Dropbox, personal drives, email attachments >10MB
Code & Repos	GitHub (company org only)	Personal GitHub, GitLab, BitBucket, USB drives
Passwords	LastPass (company account)	Browser password managers, plain text files, shared docs
Communication	Slack, Google Meet, Email	WhatsApp, Telegram, personal email for work
Customer Data	Production databases, Zendesk	Local downloads, personal machines, dev environments

Encryption Requirements:
- All laptops must have full-disk encryption enabled (BitLocker for Windows, FileVault for Mac)
- Confidential data in transit must use TLS 1.2 or higher
- Confidential data at rest must use AES-256 encryption
- USB drives containing work data must be encrypted (use company-issued encrypted drives)

Personal Devices: Confidential data must never be:
- Stored on personal computers, phones, or tablets
- Sent to personal email accounts
- Accessed from public computers (libraries, internet cafes)
- Stored on unauthorized cloud services (personal Dropbox, iCloud, etc.)

If you need to work from a personal device temporarily, contact IT for approved remote access solutions (VPN with MFA).

4. Data Retention and Disposal

ClearPath maintains data only as long as necessary for business or legal requirements:
- Employee records: 7 years after termination
- Financial records: 7 years after fiscal year end
- Customer data: Per customer contract terms (typically duration of service + 30 days)
- Email: 2 years (auto-archived)
- Slack messages: 1 year

Secure Disposal: When disposing of data or equipment:
- Use secure file deletion tools (not just 'delete' or trash)
- Old hard drives must be physically destroyed by IT (certificate of destruction provided)
- Printed confidential documents must be shredded (shredders available in all offices)
- Return all company devices to IT for proper wiping

5. Security Incident Reporting

Report security incidents immediately to security@clearpath.io. Do not attempt to investigate yourself. Examples of reportable incidents:

- Lost or stolen laptop, phone, or other device containing work data
- Suspicious emails (phishing attempts, unexpected attachments)
- Unauthorized access to systems or data
- Accidental data exposure (sent to wrong recipient, posted publicly, etc.)
- Compromised credentials (password leaked, account hacked)
- Malware or ransomware infections
- Suspicious activity in logs or alerts

Severity	Definition	Response Time	Example
Critical	Active breach or data exposure	1 hour	Customer database publicly accessible
High	Potential breach or serious vulnerability	4 hours	Phishing email with stolen credentials
Medium	Security concern without immediate risk	1 business day	Lost unencrypted laptop
Low	Minor issue or question	3 business days	Suspicious but benign email

6. Security Training

All employees must complete:

- General security awareness training within first 30 days of employment
- Annual refresher training every January
- Phishing simulation tests (quarterly)
- Role-specific training for employees accessing confidential data

Training is delivered through KnowBe4 and tracked in BambooHR. Completion is mandatory and affects performance reviews.

7. Compliance and Audits

ClearPath undergoes annual SOC 2 Type II audits. Employees may be asked to provide documentation or participate in interviews as part of these audits. Internal security audits occur quarterly.

Access logs, security events, and policy compliance are monitored continuously. Violations are investigated and may result in disciplinary action.

Questions and Support

For questions about this policy, contact:

- Security incidents: security@clearpath.io (monitored 24/7)
- Policy questions: security-team@clearpath.io
- Access requests: it@clearpath.io