Cape

Connection without compromise.

Acceptable Use Policy
Effective Date: Jun 25, 2026
Next Review Date: Jun 25, 2027
Approval Authority: Head of Security

1.0 Purpose

Cape's Acceptable Use Policy governs how personnel use Cape's technology resources, including computer equipment, software, operating systems, storage, network accounts, e-mail, and public and private internet access (collectively "systems"). These systems are intended for business purposes to serve the interests of Cape, our clients, and our customers.

2.0 Scope

This policy applies to the use of information and information systems to conduct Cape business. All personnel are responsible for exercising good judgment regarding the appropriate use of information and information systems in accordance with Cape's policies and procedures.

Effective security is a ***team effort*** that involves the participation and support of all Cape personnel who handle information and information resources. Inappropriate use exposes Cape to significant legal and operational risks, so all personnel must be aware of and adhere to this governance.

2.1 Definitions

Endpoint Detection & Response (EDR): A security capability that continuously monitors and collects endpoint data to detect, analyze, investigate, and remediate cyber threats.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Ref: NIST SP 800-53 Rev. 5 from 44 U.S.C., Sec. 3502

Mobile Device Management (MDM): The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is typically implemented through a third-party product that provides management features for specific mobile device vendors.
Ref: NIST SP 1800-21B from NIST SP 800-163 Rev.1

Multi-Factor Authentication (MFA): An authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multi-Factor Authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors.
Ref: NIST SP 800-53 Rev. 5

2.2 Table of Contents

1.0 Purpose....1
2.0 Scope....1
2.1 Definitions....1
2.2 Table of Contents....2
3.0 Policy Statement....3
3.1 General Use....3
3.1.1 Ownership....3
3.1.2 Audit & Monitoring....3
3.1.3 Onboarding & Offboarding....3
3.1.4 Reporting....3
3.2 Clean Desk....4
3.2.1 Secure Work Area....4
3.2.2 Computer Workstation....4
3.2.3 File Cabinets....4
3.2.4 Physical Keys....4
3.2.5 Passwords....4
3.2.6 Printouts....4
3.2.7 Shredders....4
3.2.8 Whiteboards....5
3.2.9 Mass Storage Devices....5
3.3 Passwords....5
3.3.1 Password Creation and Use....5
3.3.2 Password Change....5
3.3.3 Password Protection....5
3.3.4 Application Development....5
3.3.5 Multi-Factor Authentication (MFA)....6
3.4 Social Media....6
3.5 Unacceptable Use....6
3.5.1 Email and Communication Activities....7
4.0 Enforcement....9
5.0 Document Management....9

3.0 Policy Statement

3.1 General Use

3.1.1 Ownership

- All information stored on Cape's systems, regardless of whether it is owned or leased by Cape, its employees, other personnel, or third parties, remains the sole property of Cape.

- Personnel are permitted to share Cape proprietary information only when authorized by applicable law or regulation and to the extent necessary to fulfill their assigned job duties.

3.1.2 Audit & Monitoring

- For security and network maintenance, authorized personnel within Cape may monitor equipment, systems, and network traffic at any time.

- Cape reserves the right to audit systems periodically to ensure compliance with this policy.

- All day-to-day (non-testing) systems that connect to the internal network must comply with Cape's network and security requirements below, all of which are enabled by default. Users must never disable or modify these settings:
    - Device encryption must be enabled (automated via MDM)
    - A password manager must be installed and ***used*** (automated via MDM)
    - Antivirus and Malware detection software must be enabled (automated via EDR)
    - Automatic updates must be enabled (automated via MDM)
    - Screen saver and screen lock must be enabled (automated via MDM)

- Removable media may not be used with Cape systems or to store Cape information unless granted as an exception to this policy.

3.1.3 Onboarding & Offboarding

- Employees and contractors will undergo an onboarding process that familiarizes them with Cape's environments, systems, security requirements, and procedures. Employees will also receive ongoing, audited security awareness training.

- Employee and contractor offboarding will include reiterating any duties and responsibilities that remain valid after termination, verifying that access to Cape systems has been revoked, and ensuring that all company-owned assets are returned.

3.1.4 Reporting

- All personnel are responsible for promptly reporting the theft, loss, or unauthorized disclosure of Cape information or systems.

- Personnel must contact IT and Security Leadership before removing equipment, such as servers and USB devices, from the premises.

- Personnel must exercise extreme caution when opening email attachments from unknown senders. Any security violation should be reported to the Security team immediately.

3.2 Clean Desk

Cape's Clean Desk policy applies to Cape facilities and all Cape employees, contractors, and affiliates (collectively, "Personnel"). Cape's Data Classification Policy outlines applicable data designation types, including government Controlled Unclassified Information (CUI) and Cape's RESTRICTED designation, which applies to any material with access limited to a subset of personnel.

3.2.1 Secure Work Area

- Personnel must take reasonable care to physically secure any equipment assigned to them that contains Cape data (laptops, mobile devices, testing devices, etc.).

- Personnel handling government Controlled Unclassified Information (CUI) must comply with the physical safeguarding requirements defined in Cape's CMMC Physical Protection Policy and Procedures.

- Personnel shall ensure that RESTRICTED or otherwise sensitive information in hardcopy or electronic form is secured in a locked area and out of sight at the end of the day and when stepping away from their workstation.

- Personnel should take reasonable action to ensure RESTRICTED data is not viewed in an area where unauthorized personnel could oversee or "shoulder surf."

- Personnel who identify RESTRICTED or sensitive information on an unoccupied desk or elsewhere should immediately notify the Security team.

3.2.2 Computer Workstation

- Personnel shall lock workstations when leaving them unoccupied.

- Computer workstations shall have an inactivity timer of 20 minutes, after which the Screen Saver is enabled, in alignment with the CIS L2 macOS Benchmarks. Cape’s MDM platform can be used to lower this interval at any point to comply with applicable security controls.

- Computer workstations shall require a password immediately after the lock or screen saver begins, in alignment with the CIS macOS Benchmark.

3.2.3 File Cabinets

- File cabinets containing RESTRICTED or otherwise sensitive information should be kept closed and locked when not in use and when unattended.

3.2.4 Physical Keys

- Physical keys used for access to RESTRICTED or otherwise sensitive information shall not be left at an unattended desk. This includes physical keycards used to access Cape’s facilities.

3.2.5 Passwords

- Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

3.2.6 Printouts

- Printouts containing Cape RESTRICTED or otherwise sensitive information should be immediately removed from printers and fax machines. For remote printers, this includes designated INTERNAL data.

- The printing of any sensitive or controlled government data is strictly forbidden. Should such materials be found within Cape premises, the Security department must be notified immediately.

3.2.7 Shredders

- When disposing of documents, those containing RESTRICTED or sensitive information should be shredded in the official shredder bins or placed in locked, confidential disposal bins.

3.2.8 Whiteboards

- Whiteboards containing RESTRICTED or sensitive information should be immediately erased when no longer used.

- Cape personnel should take reasonable action to ensure RESTRICTED data is not viewed in an area where unauthorized personnel could oversee or “shoulder surf.”

3.2.9 Mass Storage Devices

- Mass storage devices should never be connected to Cape systems unless they have been approved by the IT and Security teams.

- If approved, mass storage devices should be treated as sensitive and securely locked.

3.3 Passwords

3.3.1 Password Creation and Use

- All users must use the company-approved password manager to securely store and manage all of their work-related passwords.

- All user-level and system-level passwords must conform to the individual account password requirements. Critical account password requirements are outlined in *Appendix A*.

- Users must use a separate, unique password for each of their work-related accounts.

- Users may not use any work-related passwords for their own personal accounts.

- User accounts with system-level privileges granted through group memberships or programs, such as “sudo,” must have a unique password that differs from all other accounts held by that user to access these privileges. Where possible, multi-factor authentication must be used on any privileged accounts.

3.3.2 Password Change

- Passwords should be changed only when there is reason to believe they have been compromised or do not meet platform password requirements.

3.3.3 Password Protection

- Individual passwords must not be shared with anyone, including supervisors and coworkers, unless used in a group account capacity.

- Password sharing shall only be done in the company-approved password management system and should be treated as RESTRICTED data per Cape’s Data Classification Policy.

- Passwords are secured using a salted password hash, along with known-good encryption.

3.3.4 Application Development

- Developers must ensure that development and production-level systems contain the following:
    - Applications must support the authentication of individual users, not groups.
    - Applications must not store passwords in clear text or in any easily reversible format.

- Applications must not transmit passwords in clear text over the network.
- Applications must provide some form of role management, such that one user can assume the functions of another without needing to know the other's password.

3.3.5 Multi-Factor Authentication (MFA)

- MFA should be used in both work and personal accounts whenever possible.

- MFA is mandated and enforced on critical systems, such as within our Identity Provider (IdP).

3.4 Social Media

- Posting from a Cape email address to newsgroups or other public forums is forbidden, unless specifically authorized by regulatory frameworks *and* in the course of business duties.

- The personal use of social media, whether on Cape's systems or personal computer systems, is also subject to the terms and restrictions outlined in this policy. Limited and occasional use of Cape's systems to engage in social media is acceptable, provided that it is done professionally and responsibly, does not otherwise violate Cape's policy, is not detrimental to Cape's best interests, and does not interfere with regular work duties. Social media usage from Cape's systems is also subject to monitoring.

- Personnel are prohibited from revealing any Cape RESTRICTED or proprietary information, trade secrets, or similar information when using social media.

- To the maximum extent allowable by law, personnel shall not engage in any social media activity that may harm or tarnish Cape and/or any of its personnel's image, reputation, and/or goodwill.

- Personnel are prohibited from making discriminatory, disparaging, defamatory, or harassing comments when using social media or engaging in any conduct prohibited by Cape's Professional Employer Organization (PEO) Company Handbook.

- Personnel may not attribute personal statements, opinions, or beliefs to Cape when participating in social media. If personnel express their beliefs and/or opinions on social media platforms, they must not, expressly or implicitly, describe themselves as representatives of Cape. Personnel assume any risks associated with such activity.

- Apart from following all laws about the handling and disclosure of copyrighted or export-controlled materials, Cape's trademarks, logos, and any other Cape intellectual property may also not be used in connection with any social media activity.

3.5 Unacceptable Use

The following activities are strictly prohibited, with no exceptions. Under no circumstances are Cape personnel authorized to engage in any illegal activity, as defined by local, state, federal, or international law, while utilizing Cape-owned or issued systems.

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Cape.

- Unauthorized copying of copyrighted material, including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Cape or the end user does not have an active license, is strictly prohibited.

- Accessing sensitive information, systems, or accounts for reasons other than conducting Cape business, as defined by your role, is prohibited, even if you may have authorized access.

- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. Management should be consulted before exporting any material that is in question.

- Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing others to use your account. This includes family members and other household members when you are at home.

- Using a Cape system to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Making fraudulent offers of products, items, or services originating from any Cape account.

- Making statements about warranty, expressly or implied, unless it is a part of regular job duties.

- Disrupting security breaches or network communications. Security breaches include, but are not limited to, accessing data of which personnel are not an intended recipient or logging into a server or account that you are not expressly authorized to access, unless these duties are within the scope of regular duties. For this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Unapproved port scanning or security scanning.

- Executing any network monitoring that will intercept data not intended for the individual's host unless this activity is a part of the personnel's regular job/duty.

- Circumventing user authentication or security of any host, network, or account.

- Introducing honeypots, honeynets, or similar technology on the Cape network.

- Interfering with or denying service to personnel (for example, denial of service attack).

- Using any program/script/command or sending messages of any kind with the intent to interfere with or disable a user's terminal session, locally or via the public or private Internet.

- Providing information about, or lists of, Cape personnel to parties outside Cape, unless part of regular job duties.

3.5.1 Email and Communication Activities

- Sending unsolicited email messages, including sending "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

- Any form of harassment via email, telephone, social media, texting, messaging, or other means, whether through language, frequency, or size of messages.

- Unauthorized use or forging of email header information.

- Solicitation of email for any email address other than that of the poster's account, with the intent to harass or to collect replies.

- Creating or forwarding "chain letters," Ponzi, or other "pyramid" schemes.

- Use of unsolicited email originating from Cape's networks or other Internet service providers on behalf of, or to advertise, any service hosted by Cape or connected via Cape's network.

4.0 Enforcement

- Cape will verify compliance with this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.
- Cape's Security and Information Technology teams must approve any exception to this policy in advance.
- Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Document Management

The Information Security team will be responsible for updating this policy at least annually or as needed. Cape personnel must review and acknowledge this policy upon hire, at least annually thereafter, and when material changes are made.

Changelog:

Rev	Rev Date	Changes	Editor	Approver	Appr Date
1.0	06/24/24	- Policy creation, requirements established - Approval Auth. delegated to Head of Security	Cameron Iati	John Doyle	07/26/24
2.0	08/06/24	- Added "!" emergency reporting section to top - Incorporated Password and Clean Desk verbiage	Cameron Iati	Patrick Ballard	08/14/24
2.1	06/02/25	- Moved emergency reporting to IRP - minor Password Protection updates	Cameron Iati	Alek Amrani	06/03/25
2.2	10/15/25	- Format updates	Cameron Iati	Alek Amrani	10/16/25
2.3	05/04/26	- Added government controlled language to Safe Desk section for CMMC framework	Cameron Iati	Alek Amrani	05/04/26
2.4	06/25/26	- Added prohibition on printing controlled government information to Printouts section	Cameron Iati	Alek Amrani	06/25/26