Captiva Erosion Prevention District

Information Technology Security Plan

Working Draft

Prepared for CEPD use with CMIT Solutions serving as outsourced IT support provider and custodian of administrative/master credentials, excluding individual banking credentials.

Adopted by:	Captiva Erosion Prevention District
Approval Date:	
Effective Date:	
Reviewed by:	CEPD / CMIT / District Counsel, as needed
Next Review:	Annually or upon material system, staffing, vendor, or legal changes

Note: This plan is an administrative security document and should be reviewed by District counsel for legal sufficiency and consistency with CEPD policies and contracts.

1. Purpose

The purpose of this Information Technology Security Plan is to protect CEPD electronic records, systems, accounts, devices, passwords, financial information, public records, and operational data from unauthorized access, loss, misuse, disclosure, or disruption.

This plan establishes procedures for access control, password management, vendor oversight, backups, cybersecurity training, incident response, and continuity of operations.

CEPD relies on CMIT Solutions as its outsourced IT support provider. CMIT is authorized to manage CEPD IT systems, security tools, devices, user access, and administrative/master credentials, subject to District oversight and this plan. Banking credentials are specifically excluded from CMIT password custody and may only be known to the individual authorized banking users.

2. Scope

This plan applies to CEPD employees, board members, contractors, consultants, and vendors who access CEPD systems or data.

This plan applies to CEPD email accounts, Microsoft 365/Teams, shared drives, cloud storage, computers, phones, tablets, printers, websites, accounting systems, payroll systems, banking access, public-records storage, and any other District technology.

This plan also applies to CMIT and any subcontractors or tools used by CMIT to support CEPD technology.

3. IT Support and Responsibility

CMIT shall serve as CEPD primary IT support provider and shall be responsible for managing CEPD devices, user accounts, network access, endpoint protection, security updates, onboarding, offboarding, backups, and incident-response support.

CMIT is authorized to hold and maintain administrative/master passwords in a secure password-management system, except for individual banking credentials.

CEPD remains responsible for governance and oversight. CMIT should not be the only party with practical knowledge of where District credentials, records, and systems are located.

4. Administrative and Master Password Control

CMIT may hold administrative/master credentials for CEPD systems, but those credentials must be stored and managed using reasonable security controls. Individual banking credentials are excluded from CMIT password custody.

All non-banking administrative/master credentials and related system-control information are District assets. Any current or former IT consultant or vendor must transfer such access to CEPD or CMIT upon District request so the District is not locked out of its own systems.

All administrative, master, shared, vendor, and emergency credentials, other than banking credentials, must be stored in a secure password-management system controlled by CMIT, with appropriate CEPD ownership or recoverability. Banking credentials must remain accessible only to the specific CEPD-authorized banking users assigned those credentials.

Passwords must not be stored in email, text messages, sticky notes, unsecured spreadsheets, Word documents, or personal browser password managers.

CEPD shall maintain a sealed or otherwise secured emergency-access procedure for critical non-banking credentials. Staff should not routinely use master passwords, but CEPD must not be locked out of its own systems if a vendor relationship changes or an emergency occurs. Banking access recovery must follow the financial institution authorized-user process rather than sharing or vaulting individual banking passwords.

Whenever possible, individual user accounts must be assigned rather than shared logins. Shared credentials should be limited to situations where a system does not support individual users.

Administrative/master passwords must be reviewed and changed when CMIT assumes support from a prior vendor, a key staff member or vendor separates, a password is suspected to be exposed, an account has been accessed by an unauthorized person, or a vendor relationship ends.

CMIT shall provide CEPD with a periodic list of active users and administrative accounts for review, without disclosing passwords in an unsafe manner.

5. Multi-Factor Authentication

Multi-factor authentication should be enabled on all systems that support it, including Microsoft 365/Outlook/Teams, banking access, payroll systems, accounting systems, website administrator accounts, cloud storage, password managers, remote-access tools, and accounts with access to District records or financial information. Banking MFA devices, codes, tokens, or authenticator access must not be shared with CMIT or any other unauthorized person.

MFA must be required for administrative accounts whenever available.

Where feasible, CMIT should use phishing-resistant MFA or stronger authentication methods for administrative accounts.

6. User Access and Permissions

Access shall be based on the principle of least privilege. Users should only have access to the systems and files necessary to perform their assigned duties.

CMIT shall assist CEPD with creating user accounts, assigning permissions, removing access promptly when users leave, reviewing permissions periodically, disabling unused accounts, and separating administrative access from regular user access.

Board members, staff, consultants, and vendors should not use personal email accounts for official CEPD business unless specifically authorized and properly preserved for public-records purposes.

7. Onboarding Procedure

Before a new employee, board member, contractor, or vendor receives access to CEPD systems, CEPD or CMIT shall confirm that the person has a legitimate business need for access and that the correct systems and permission levels have been identified.

MFA must be enabled where available before access is issued.

New users should receive basic cybersecurity and public-records guidance and should understand not to share passwords or forward District records to unauthorized accounts.

8. Offboarding Procedure

When an employee, board member, contractor, consultant, or vendor no longer requires access, CEPD shall notify CMIT immediately.

CMIT shall disable or remove email, Microsoft 365, Teams, shared-drive, VPN, remote-access, financial-system, website, and cloud-system access as applicable.

CMIT shall recover District devices, files, and records when applicable; change shared passwords if the person had access to them; preserve District records according to public-records and retention requirements; and document completion of the offboarding process.

Offboarding should occur the same day CEPD knows access is no longer authorized, especially for financial, administrative, or sensitive accounts.

9. Device Security

All CEPD-owned computers, tablets, phones, and other devices should be managed or monitored by CMIT to the extent practical.

Minimum safeguards should include password or PIN protection, automatic screen lock, current operating system updates, endpoint protection, encryption where available, remote wipe or lock capability where feasible, no unauthorized software installations, and separation of personal and District data where possible.

Personal devices used for CEPD business should be limited and should not be used to store District records unless approved and properly backed up or preserved.

10. Email, Teams, and Cloud Storage

CMIT shall assist CEPD in securing Microsoft 365, email, Teams, OneDrive, SharePoint, or other cloud platforms.

Controls should include MFA, spam/phishing protection, review of external sharing permissions, restrictions on automatic forwarding to personal email, appropriate retention and backup settings, use of shared folders or Teams channels instead of personal storage for District records, and periodic review of former users, guest users, and external sharing links.

Users should be trained to report suspicious emails, unexpected attachments, payment-change requests, fake invoices, unusual login prompts, or requests to bypass normal procedures.

11. Financial and Banking Security

Banking credentials must not be stored in any CMIT password vault, District shared password vault, shared file, email, text message, browser password manager, or other location accessible to anyone other than the specific CEPD-authorized user assigned those credentials.

Each authorized banking user must have a separate user ID and password whenever the financial institution supports individual access. Shared banking credentials are prohibited unless the bank provides no individual-user option and CEPD approves an exception in writing.

Banking passwords, MFA codes, security questions, tokens, authenticator apps, and recovery methods must not be disclosed to CMIT, other vendors, other staff, board members, or any person who is not the assigned authorized banking user.

CMIT may assist with device security, browser security, malware protection, phishing response, and general technical support for banking access, but CMIT shall not view, store, request, reset for its own use, or retain individual banking credentials.

Access to banking platforms shall be granted, changed, or removed only through the financial institution authorized-user process and approved CEPD procedures.

Payment changes, vendor banking changes, ACH setup, wire transfers, and unusual payment requests should require independent verification and any approvals required by CEPD policy.

Access to payroll, accounting, and banking platforms should be reviewed regularly, and banking access should be removed promptly when a user is no longer authorized.

12. Backups and Recovery

CMIT shall ensure that CEPD has appropriate backup and recovery procedures for critical systems and records.

Backups should cover Microsoft 365/email where feasible, shared files and cloud storage, key District records, website data if applicable, financial/accounting data where applicable, and locally stored data on District devices if any.

Backups should be protected from deletion, ransomware, or unauthorized alteration. Backup restoration should be tested periodically.

13. Records Retention and Public Records

Because CEPD is a public agency, IT practices must support Florida public-records obligations.

District records should be stored in approved District systems whenever possible. Staff, board members, consultants, and vendors should avoid storing official District records only on personal devices, personal email accounts, or individual-only accounts.

CMIT shall assist CEPD in preserving access to electronic records during staff transitions, vendor changes, device replacements, or account closures.

This plan does not replace CEPD public-records policy or legal advice from District counsel.

14. Cybersecurity Training

All CEPD users with access to District systems should complete cybersecurity training upon onboarding and annually thereafter.

Training should include phishing and suspicious email recognition, password and MFA requirements, safe handling of attachments and links, public Wi-Fi and remote-work risks, proper storage of District records, reporting lost devices or suspected incidents, avoiding unauthorized software or browser extensions, and financial fraud/vendor-payment-change scams.

15. Vendor and Contractor Access

Vendors, contractors, consultants, and IT service providers serve at the will and direction of the District. No vendor, contractor, consultant, or former service provider owns, controls, or may withhold CEPD accounts, credentials, records, software access, domain access, email administration, cloud storage access, website access, device access, backup access, security tools, or other District technology assets.

All access granted to a vendor or consultant is for the limited purpose of performing District-approved work and may be modified, suspended, or terminated by CEPD at any time. Vendors and consultants shall only receive the minimum access necessary to perform authorized services.

Upon request by CEPD, its District Manager or designee, District counsel, the Board, or CMIT as the District's authorized IT support provider, any current or former vendor, contractor, consultant, or IT provider must promptly return, transfer, disclose, or otherwise provide to the District all District-owned access information and administrative control necessary for CEPD to operate and secure its systems.

Required turnover includes, as applicable, administrator usernames, passwords, MFA recovery methods, recovery codes, domain registrar access, DNS access, website hosting access, Microsoft 365/Google/cloud administration, device-management tools, backup systems, security tools, software license portals, documentation, configuration records, and any other credentials or system information related to District business.

No vendor or consultant may use possession of credentials, systems, records, or administrative access to delay transition, restrict District operations, prevent CMIT from performing authorized support, or condition turnover on additional approvals not required by the District. Turnover must occur promptly upon District request and in a secure manner approved by CEPD or CMIT.

Before access is granted, CEPD and CMIT should confirm the business need for access, whether access should be temporary or ongoing, what systems or records the vendor may access, whether MFA is enabled, and whether the vendor must comply with confidentiality, public-records, cybersecurity, transition, and credential-turnover requirements.

Vendor access should be removed promptly when the work ends or when CEPD determines the access is no longer authorized. CMIT should maintain a list of vendors with access to CEPD systems, including the type of access granted and whether access has been disabled or transferred.

16. Incident Response

A cybersecurity incident may include a suspected hacked email account, lost or stolen device, ransomware or malware alert, unauthorized access to District files, fraudulent invoice or payment-change request, suspicious login activity, accidental disclosure of sensitive information, or a former vendor or employee retaining unauthorized access.

If an incident is suspected, CEPD users should immediately notify CMIT and the District Manager or designated CEPD contact.

CMIT shall assist with securing affected accounts or devices, resetting passwords, reviewing logs where available, preserving relevant records, determining whether other systems were affected, restoring data if needed, documenting actions taken, and recommending whether District counsel, insurance, law enforcement, banking institutions, or state cybersecurity contacts should be notified.

17. Remote Access

Remote access to CEPD systems shall be limited, secured, and approved.

Remote access should require MFA, secure remote-management tools approved by CMIT, no unauthorized remote desktop software, logging where feasible, and immediate removal when no longer needed.

Administrative remote access should be limited to CMIT or other approved vendors.

18. Website and Domain Security

CMIT or another approved provider shall help CEPD maintain secure control over the CEPD domain name registration, DNS records, website administrator accounts, website hosting credentials, SSL certificates, and website backup and recovery information.

Domain, DNS, and website administrator credentials are critical District assets and should be stored in the CMIT password vault with CEPD emergency recovery capability.

19. Annual Review

At least annually, CEPD and CMIT should review active users, administrative accounts, vendor access, password vault structure, MFA status, backup status, device inventory, software and license inventory, cybersecurity training completion, incident history, and any needed improvements.

20. CMIT Reporting to CEPD

CMIT should provide CEPD with periodic or annual documentation sufficient for oversight, including active users, administrative accounts, confirmation that master credentials are stored securely, MFA status for major systems, backup status and last test date if applicable, device inventory, known security issues or recommended improvements, and confirmation of completed onboarding/offboarding requests.

21. Cybersecurity Standards

CEPD should maintain cybersecurity practices consistent with generally accepted best practices, including applicable NIST and CISA guidance, and should review legal obligations with District counsel.

22. Approval and Maintenance

This IT Security Plan should be reviewed by CEPD administration, CMIT, and District counsel as needed.

Once approved, the plan should be reviewed annually or whenever there is a significant change in IT provider, District systems, staffing, financial platforms, legal requirements, cybersecurity risk, or incident history.

Implementation Checklist

Item	Responsible Party	Status/Notes
CMIT confirmed as IT administrator	CEPD / CMIT	
Master passwords stored in secure vault, excluding individual banking credentials	CMIT	
CEPD emergency access procedure documented	CEPD / CMIT	
MFA enabled on Microsoft 365	CMIT	
MFA enabled on banking/accounting/payroll systems	CEPD / CMIT, with banking credentials restricted to authorized users only	
Active user list reviewed	CEPD / CMIT	
Former users removed	CMIT	
Vendor access reviewed	CEPD / CMIT	
Device inventory completed	CMIT	
Backup process documented	CMIT	
Backup restoration tested	CMIT	
Cybersecurity training completed	CEPD	
Incident-response contact list created	CEPD / CMIT	
Website/domain credentials secured	CMIT	
Annual review scheduled	CEPD	

Suggested Board Motion

Motion to approve the Captiva Erosion Prevention District Information Technology Security Plan, recognizing CMIT Solutions as the District outsourced IT support provider and custodian of administrative/master credentials, excluding individual banking credentials, subject to District oversight, access controls, cybersecurity training, backup procedures, incident-response protocols, and annual review.

Reference Notes

- Florida Statutes, section 282.3185, Local Government Cybersecurity, including cybersecurity training and standards provisions.
- NIST Cybersecurity Basics, including recommendations for MFA, password managers, backups, and changing default passwords.
- CISA Cross-Sector Cybersecurity Performance Goals and CISA small and medium business cybersecurity resources.
- Florida Statutes, Chapter 119, Public Records, including provisions related to access to automated/electronic public records.

These references are included for planning context only. CEPD should consult District counsel regarding legal requirements applicable to the District.