DUTCHESS COUNTY-POUGHKEEPSIE
LAND BANK

Information Technology Policy

Introduction

This Information Technology (IT) Policy outlines the acceptable use of technology resources provided by the Dutchess County-Poughkeepsie Land Bank (DCPLB). These resources are intended to support the organization's mission. By using these resources, you agree to abide by this policy.

Acceptable Use

- Technology resources are for conducting official DCPLB business only. Incidental personal use is permitted, but it must not interfere with work duties or consume excessive resources.
- Downloading or installing unauthorized software is strictly prohibited. Only approved software may be used.
- Sharing of login credentials with others is strictly prohibited. Each user is responsible for the security of their own account and activity.
- Sending or receiving inappropriate or illegal content (e.g., offensive, discriminatory, copyrighted material) is forbidden.
- Engaging in activities that could compromise network security (e.g., hacking, peer-to-peer file sharing) is strictly prohibited.

Authentication and Passwords

- Strong passwords are required. A strong password is at least 12 characters long and includes a combination of uppercase and lowercase letters, numbers, and symbols.
- Passwords should not be easily guessable (e.g., birthdays, pet names, dictionary words).
- Users are required to change their passwords upon initial login and periodically thereafter.
- Multi-factor authentication (MFA) should be used when available. MFA provides an additional layer of security by requiring a second verification step during login (e.g., code from a mobile app).

Acceptable Software Use

- Only software approved by the Executive Director may be installed or used on DCPLB devices. Users should request approval for any new software through the Executive Director.
- Downloading software from unauthorized sources is strictly prohibited.
- Freeware and open-source software may be used only with prior approval.

Adopted April 30, 2025

Email Usage

- Email accounts are provided for official business communication only. Personal use should be minimal and not interfere with work duties.
- Users are responsible for maintaining a professional tone in all email communications.
- Do not share sensitive information via unencrypted email, especially when using public Wi-Fi.
- Be cautious about opening attachments from unknown senders or clicking on suspicious links within emails. Phishing attempts are common.

Social Media Usage

- While official DCPLB social media accounts exist, employees are not expected to use personal accounts for work purposes unless explicitly authorized by their supervisor.
- When engaging with DCPLB-related topics on personal social media accounts, employees are encouraged to be professional and avoid disclosing confidential information.

Remote Access

- Remote access to DCPLB resources may be granted to authorized personnel for work purposes only.
- Users are responsible for securing their remote access connections and immediately reporting any suspected compromises.
- Additional security measures for remote access, such as requiring specific VPN software may be required.

Mobile Device Usage

- DCPLB-issued mobile devices are for work purposes only.
- Users are responsible for the security of their mobile devices and should enable features like screen locks and data encryption.
- Lost or stolen mobile devices should be reported immediately to the Executive Director.
- Personal data stored on mobile devices should be minimized, and sensitive information should not be accessed on public Wi-Fi networks without a VPN.

Data Security

- Users are responsible for safeguarding confidential information, including client data, financial records, and internal documents.
- Data should not be transferred or stored on unauthorized devices or cloud storage services.

- Report any suspected data breaches or security incidents immediately to the Executive Director or designated personnel.

Consequences of Policy Violation

Violations of this policy may result in disciplinary action, up to and including termination of employment or volunteer privileges.

Review and Updates

This policy is subject to review and updates at any time. We encourage users to periodically review this policy for any changes.

Disaster Recovery Policy

Purpose

This policy outlines the procedures for the Dutchess County-Poughkeepsie Land Bank (DCPLB) to recover critical data and resume operations following a disaster. A disaster is any event that significantly disrupts normal operations, such as fire, flood, power outage, cyberattack, or natural disaster.

Scope

This policy applies to all DCPLB employees, volunteers, and IT systems containing critical data. Critical data includes:

- Property information (addresses, titles, deeds)
- Financial records (budgets, grants, donor information)
- Client and partner contact information
- Operational documents (policies, procedures, meeting minutes)

Risk Assessment

The DCPLB will conduct a periodic risk assessment to identify potential threats and vulnerabilities to its critical data.

Backups

- All critical data will be backed up regularly (at least weekly) to a secure offsite location, such as a cloud storage service.
- Backup copies will be verified periodically to ensure they are complete and usable.

Recovery Procedures

- In the event of a disaster, the DCPLB will follow these steps:
  - Assess the situation and ensure the safety of staff and volunteers.
  - Identify the critical systems and data needed for recovery.

  - Restore critical data from backups.
  - Resume essential operations as quickly as possible.
  - Document lessons learned from the disaster to improve future preparedness.

Roles and Responsibilities

- The Executive Director is responsible for overseeing the development, implementation, and testing of this policy.
- The Executive Director or their designee is responsible for maintaining backups and ensuring their functionality.
- All staff and volunteers are responsible for reporting any potential threats or disruptions to critical data.

Testing and Training

- This policy will be reviewed and updated annually.
- Disaster recovery procedures will be tested periodically to ensure their effectiveness.
- Staff and volunteers will be trained on their roles and responsibilities in the event of a disaster.

Communication

- In the event of a disaster, the DCPLB will communicate with staff, volunteers, and stakeholders regarding the status of operations and recovery efforts.

Limitations

This policy is intended to provide a basic framework for disaster recovery. The DCPLB acknowledges that resources are limited for a small non-profit. It is recommended to prioritize the most critical data and functionalities for recovery within available resources.