VERMONT BOND BANK CYBER SECURITY POLICY

Adopted: February 15, 2012
Revised: December 18th, 2018
Revised: June 25th, 2020

Scope: This policy covers employee security procedures related to computer, network security, and electronic transfer of sensitive information.

Purpose

This policy is intended to protect the integrity of the Vermont Bond Bank ("Bond Bank") network, to mitigate the risks and losses associated with security threats to computing resources and to ensure secure and reliable network access and performance. This policy is necessary to provide a reliable campus network to conduct the Bond Bank's business and prevent unauthorized access to Bond Bank data. In addition, the Bond Bank has a legal responsibility to secure its computers and networks from misuse.

SCOPE

The scope of this policy includes all personnel and consultants who have or are responsible for an account (or any form of access that supports or requires a password) on any network system for which the Bond Bank is the primary administrator. All devices that may access a Bond Bank network fall under the scope of this policy.

SECURITY RESPONSIBILITIES

The responsibility for cyber security falls upon all employees and users of the Bond Bank's network systems. The Bond Bank's network systems are cloud based and accessible through login information. Therefore, the primary source of potential disruption revolves around compromised login security.

Additionally, non-network compromise may occur through imposter or false representations via electronic means that seek to criminally make use of Bond Bank resources.

In both above cases, the lynchpin of protection is the diligence of employees to follow password protocols and report suspicious activity.

REPORTING

All potential suspicious activity or compromises to the Bond Bank's network should be reported to the Executive Director. In the absence of the Executive Director, suspicious behavior should be reported to the Tech Group (cloud / network), Hark (vtbondbank.org website), or NewBreed (vehbfa.org website).

PHYSCIAL SECURITY

Bond Bank employees should always be present in the office when outside or unverified parties are within the office. The Bond Bank will rely upon provider security protocols for server and data storage security after review with the Bond Bank’s technical consultants.

NETWORK REDUDENCY

The Bond Bank will employ management of network resources to ensure that information is backed up through multiple unrelated services at server locations that do not overlap.

NETWORK LOGIN SECURITY

All system-level passwords will be reset at the prompting of the system administrator every 60 days. New logins require two step verification.

Password Construction Guidelines

All users at the Bond should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Punctuation
    - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
    - Contain at least nine alphanumeric characters.
- Weak passwords have the following characteristics:
    - The password contains less than nine characters
    - The password is a word found in a dictionary (English or foreign)
    - The password is a common usage word such as:
        - Names of family, pets, friends, co-workers, fantasy characters, etc.
        - Computer terms and names, commands, sites, companies, hardware, software.
        - The words "Vermont Bond Bank, "vbb", or any derivation.
        - Birthdays and other personal information such as addresses and phone numbers.
        - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
        - Any of the above spelled backwards.
        - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

(NOTE: Do not use either of these examples as passwords!)

Password Protection Standards

- Do not share Bond Bank passwords with non-employees. All passwords are to be treated as sensitive, confidential information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Executive Director.
- Always decline the use of the "Remember Password" feature of applications.

TRANSFER OF SENSITIVE INFORMATION

The Bond Bank's staff and consultants transferring sensitive information will use a secure means to transmit electronic information (currently through the Barracuda network service). In the event this cannot be accessed, sensitive information will be exchanged via facsimile.

INFORMATION AVAILABLE ON WEBSITE

Any information made available through the Bond Bank's website (vtbondbank.org) regardless of whether it can only be accessed via password, including but not limited to, municipal loan applications, shall be redacted to remove any and all information related to bank accounts (name, account, and routing numbers) and personal information (name, Social Security number, driver's license or state-issued ID number, credit/debit card or other financial information)

USE OF PERSONAL ELECTRONIC DEVICES

Employees who use their own personal electronic devices (cellular phone, tablet, laptop, desktop computer) for Bond Bank business purposes must adhere to the following guidelines:

1. Employees must take reasonable steps to install or otherwise ensure security of their devices;
2. Employees will exercise caution when installing third party applications on their devices, as they may exploit vulnerabilities that could expose confidential Bond Bank information and data;
3. Employees must limit access to their devices from those who are not authorized to it, including family members, friends, associates and colleagues;
4. The Bond Bank reserves the right to access an employee' s device at any time to examine items related to its matters; to implement security controls; to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings; or to check for/monitor compliance with Bond Bank policies and procedures;
5. If a device is lost or stolen, the employee must contact the Executive Director immediately, so the Bond Bank can take appropriate actions;
6. Non-exempt employees should adhere to their current hours of employment and should not use their devices for business purposes outside of those hours, unless prior approval is obtained from the Executive Director;
7. At the conclusion of employment, the Bond Bank will either inspect a departing employee' s device to ensure that it is free of Bond Bank data, wipe the employee' s device clean of all data, or otherwise ensure no proprietary information is retained on a personal device.

The Bond Bank’s policies and rules of behavior regarding the use and/or access of organizational e-mail and other Bond Bank systems and/or services apply to an employee’ s use of any device and remain in effect at all times.

MONIORING

The Bond Bank has the right to monitor all employee and user activity of network systems to ensure compliance with this Cyber Security Policy. Employees / users should have no expectation of privacy when using Bond Bank computers and/or network systems.

REVIEW

This policy will be reviewed by the Bond Bank annually or upon any proposal to make additional information available on the Bond Bank’s website.