Distributable cleverDome Cybersecurity Package

Table of Contents

0. INTRODUCTION: CLEVERDOME

0.1 cleverDome Business Overview

cleverDome aims to implement and easily provision essential elements of the security ecosystem that are often difficult for all to implement and effectively manage.

- **Secure Devices – Providing Safe Easy Access to the Secure Network via Approved Endpoint Protection Providers:** Entry to the Dome is restricted to secure devices, i.e. devices with end point protection in place with 24/7 monitoring. End users don't need to learn anything new, just access it normally through a web browser or a SSH client. Access to the Dome is controlled through a provisioning process to determine which cleverDome members can access which services on which servers of other cleverDome Members. As of November 2017, Entreda and ProtectIT (a service leveraging Sophos provided by Financial Computer) are the two currently approved end point gateway providers.

- **Member Risk Management – Cybersecurity Due Diligence:** cleverDome acts as a trust broker by provisioning cleverDome members to exchange confidential data. Each member is required to meet minimum cybersecurity standards and complete the due diligence process to enter the Dome. cleverDome members benefit from the common standards and shared due diligence.

- **Private, Secure Network:** Information is protected by a private internet where the data goes through a specially configured cloud directly to the destination point using military grade cybersecurity. The data is fractionalized and dispersed over multiple channels. The result is a private network that is safe, reliable and faster than a VPN connection.

For a more detailed overview, contact cleverDome.

1. CLEVERDOME CYBERSECURITY PROGRAM

1.1 Program Overview

cleverDome's Cybersecurity Program includes:

- Conducting and documenting a periodic risk assessment to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information and personal information systems that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information or systems.
- Designing and implementing adequate written policies and procedures and other safeguards to control the risks identified.
- Regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures.
- Responding to unauthorized access of personal information, investigating the extent of the incident, containing the incident, and taking steps to prevent further unauthorized access.
- Overseeing vendors / service providers, and documenting the oversight conducted.

cleverDome employs a professional Managed Security Services Provider (MSSP), Financial Computer. Our relationship with Financial Computer results in 24x7x365 cyber monitoring, active threat mitigation, and assists to implement processes and technical controls in the areas of:

- Access Rights and Controls
- Data Loss Prevention
- Vendor Management
- Training
- Incident Response

When designing our cybersecurity program, a tailored list of actions and controls discussed in this document assist to create a "series of mechanisms" most suitable to our organization and those that we serve (i.e. a castled approach to protection). Specifically, that our organization employs Cyber Monitoring, Managed Antivirus, Managed Encryption, Secure Messaging, Two Factor Authentication and Encrypted Backups on our devices where applicable. Simultaneously, as the manager of a secure, private network we also enable our member organization to achieve secure devices, secure communications, and verifiable cybersecurity due diligence on all members.

Risk Assessments for the firm will be performed routinely (and some components such as technical vulnerability scanning more often and some such as active threat monitoring continuously). The assessment process includes:

- ✓ Vulnerability scanning to identify and document asset vulnerabilities
- ✓ Review threat and vulnerability information from information sharing forums and sources
- ✓ Identify and document internal and external threats
- ✓ Identify potential business impacts and likelihoods
- ✓ Use threats, vulnerabilities, likelihoods and impacts to determine risk
- ✓ Identify and prioritize risk responses.

1.2 Essential Technical Controls Summary

Below is a status of essential technical controls in order for compliance (e.g. with NY-DFS and FINRA/OCIE guidance) and enforcement of essential protections.

Essential Technical Control	Compliant & Enforced*
Automated Critical Asset Inventory Auditing / Cyber Monitoring**	Yes
Operating Systems (OS) in Compliance with Minimum Standards	Yes
Devices in Compliance with Minimum Standards	Yes
Full Disk Encryption (FDE) on All Devices	Yes
Anti-Virus / Anti-Malware w/ Automated Patching and Updates	Yes
Secure Messaging / Email Encryption and Filtering	Yes
Encrypted Full Image Backups	Yes
Multi-Factor Authentication (MFA) for Remote Access to Network***	Yes

(*) Compliant: Cyber Monitoring Exits to Evidence Control Status; Enforced: Out of Compliance Users / Devices Electronically Remediated.

(**) Automated auditing results in real-time notification re: the state of fundamental cyber protections (e.g. FDE, firewall, password complexity, screen saver timeout / security, AV/AM status, etc.).

(***) MFA required for remote access to network / devices. MFA also used to protect against unauthorized access to Nonpublic Information or Information Systems (even within the network – i.e. MFA used to access any cleverDome device).

1.3 Elements Addressed in cleverDome's Cybersecurity Program

2. TECHNICAL CONTROLS

2.1 Minimum Security Standards and Technical Controls Overview

All advisors and devices accessing the Dome need to meet minimum security standards. Simultaneously, cleverDome employees are subject to the same minimum security standards.

Identity / Access Provisions:

Multi-Factor Authentication: Access to the Dome requires provisioned devices to utilize multi-factor authentication.

Passwords: Temporary passwords must always be changed. Each person accessing the Dome must have their own unique user ID and password. Passwords used to access the Dome must be strong passwords. Specifically,

- Passwords must not contain the UserID.
- Passwords must be at least eight (8) characters long.
- Passwords must be case sensitive (i.e., uppercase/lowercase letters are separate and distinct).
- Passwords must contain characters from at least two of the following four sets:
  - uppercase letters ('A' through 'Z').
  - lowercase letters ('a' through 'z').
  - numerals ('0' through '9').
  - punctuation characters ('.', '!'. '#', '?', '>', '+', etc.).
- Systems and applications must require the user to change their password a minimum of every 90 days or force users to re-authenticate / revalidate their security challenge questions or image minimum of every 90 days.

Mobile Devices should adhere to the following password guidelines:

- Password length = 6-character minimum.
- Password Complexity = Minimum of 1 alpha and 1 numeric character.
- For iPads and iPhones = 6 Characters Passcode (Simple passcode OFF), and/or optional
- Apple Touch ID fingerprint enrollment where available.

Lock Screens: Systems should be configured to lock, and require re-login after a period of 30 minutes of inactivity.

Users: Systems used for business should only EVER be used for business and by persons that are using it/them to conduct business, no other use of the systems should/will be permitted.

Operating Systems (OS):

Desktops/Laptops: Computers should be within full/extended support period from OS Vendor

Current Microsoft Desktop OS's: Windows 7, Windows 8, Windows 8.1, Windows 10 (x86, 32-bit and 64-bit).

Current Apple Desktop OS's: Mac OS X 10.8 (Mountain Lion), Mac OS X 10.9 (Mavericks), Mac OS X 10.10 (Yosemite), Mac OS X 10.11 (El Capitan)

Mobile Devices:

IOS (9 or later)

Android (4 or later)

Servers: Servers should be within full/extended support period from OS Vendor

Current Microsoft Server OS's: Windows Server 2008, Windows SBS 2008, Windows SBS 2011, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016

Systems that do not meet the above operating system requirements must be upgraded immediately to a supported operating system, or their use immediately discontinued.

Hardware:

CPU: 1.5 GHz x86 (64 bit preferred)

RAM: 4 GB (minimum); 8 GB preferred

Available Hard Disk Space: 250 MB

Operating System Updates/Patches:

Desktops/Laptops: Operating systems, browsers and applications must be configured to automatically check for, download, and install security updates when available and be on vendor supported versions of the software. For systems that are not monitored/maintained by an in-house or third party IT department, automatic updates must be enabled. Computer systems such as laptops and desktop computers must have a software firewall enabled to block all traffic to the system that is not required to perform and use business software.

Servers: Patches must be applied and the system rebooted at least monthly. Must be configured in accordance with documented standards / procedures that are based on a generally accepted and authoritative source of security configuration information (e.g., Microsoft). Server configurations must be examined periodically to ensure that they continue to meet their documented configuration standards. Servers must have disk-level encryption. Systems must be patched regularly with the latest security updates. For systems that are not monitored/maintained by an in-house or third party IT department, automatic updates must be enabled.

System Protection Software:

Anti-Virus / Anti-Malware: Anti-virus and anti-malware software must be installed and be operationally enabled as part of each computer's start-up process. (e.g., servers, desktops, laptops, etc.) and configured, at a minimum to:

- Prevent and/or block viruses and other malicious programs (e.g., malware) from infecting the computer system; and
- Automatically check for, download and install updates.

Encryption Best Practices Guidance:

Devices connected to the Dome must employ full disk encryption.

Device: Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Approved full disk encryption vendors should be installed on all endpoint devices.

Connections: Encrypting your connections secures communication between your device and others devices (e.g. over a computer network, to the internet). Best practice guidelines include:

- Secure connections and protocols (e.g. HTTPS, TLS) should always be used.
- Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with Wi-Fi Protected Access 2 (WPA2) protection.

- Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol---Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.

Add section re: technical tools that matches

Note: The balance of details in section 3, 4, & 5 have been removed for confidentiality / security reasons. For a verbal review of related policies / procedures, contact us to arrange a discussion.

2.1.1 For Additional Information

Caution is exercised in sharing information regarding the breadth, depth, and maturity of cleverDome's information security program and technical controls. For a more detailed, confidential walkthrough of cleverDome policies & procedures and technical controls, please contact Michael Hallet at michael.hallett@cleverdome.com or by calling (650) 888-8728. Upon completing a NDA, a confidential discussion will be scheduled.