Rehoboth Information Technology Advisory Committee Meeting Minutes

Date of Meeting: 9 November 2022

Meeting Location: Francis Farm, Arcade Bldg.

Members of Committee:	**In Attendance:**
Anna Deignan (AD) (Chair)	Present
Tim Maynard (TM) (Secretary)	Present
Jay Jil (JJ)	Present
Reuben Fishman (RF)	Absent

Official Observers: George Solas

Old Business:

Jay Jil moved to approve the minutes of the IT meeting of October 26, 2022 (draft 3). The motion was seconded by Tim Maynard and passed unanimously.

Anna Deignan announced that the Board of Selectmen has approved the I.T. Committee Charter as received from the town's legal advisors. We will finalize and publish it. Anna will clean it up and we will all sign it at a date in the near future.

With regard to the questions that the committee has sent to Derek Rousseau (Town IT Director), he sent an incomplete list of answers to Anna. Anna would like the committee to provide him with a comprehensive list of our concerns. It was announced that Derek would be going on three months of paternity leave commencing at the end of this month. Anna made it clear that she provided Derek with a list of the committees concerns (on 9/13/2022) and let him know that we are willing to provide assistance to him. Anna's list will be included in the minutes by attachment.

The committee reviewed the RFP proposed by the Board of Selectmen. It appeared to be fine but a starting point and end point is needed to further refine the scope. Anna suggested that she talk to Derek (for 2 to 3 hours) to review with the eye to developing a framework to follow for the RFP. This will better define our environment. George agreed that it was a good idea and will review it with the Board of Selectmen to receive their "buy in".

Relative to the "Security Awareness/Elder Fraud" presentation for the C.O.A., the development is ongoing and it is scheduled for Monday, November 28, 2022 at 1:00 pm at the C.O.A. building.

New Business:

A discussion was undertaken by the committee relative to meeting frequency and the upcoming holidays. Tim Maynard made the motion to revert back to monthly meetings in the Arcade Building starting December 14, 2022 (2nd Wednesdays) until further notice. It was seconded by Jay Jil and passed unanimously.

Motion:	**Presented By:**	**2nd:**	**Vote:**
Move to adjourn (at 8:19 pm)	Tim Maynard	Jay Jil	passed unanimously

---------- Forwarded message ---------
From: **Anna Deignan** <anna.m.deignan@gmail.com>
Date: Tue, Sep 13, 2022 at 2:35 PM
Subject: IT Compliance - Lists and Actions
To: Derek Rousseau <drousseau@rehobothma.gov>

Hi Derek,

I'm sorry this is delayed. Work has been something else since my return.
Below is a list of items and actions that *should* ideally be done for any environment, to protect assets. Sorry if it seems like a lot and I'm sure I've missed something. This is really to get you thinking about areas you might want to address sooner rather than later.

My hope is that the committee can eventually help with any of these that are more urgent to document (such as inventories). The rest will probably remain "nice to have but not possible for the foreseeable future..."

- Document architecture: policies, standards, and procedures (currently on our to-do list). Kept up-to-date, reviewed each year with sign-off, and updated as necessary.
- "Enterprise" asset inventory: Inventory, track, and maintain a detailed list of all assets including end-user devices, portable and mobile, network devices, IoT devices, and servers (both physical and virtual, on-prem and in cloud). Details to track should include network address (if static), hardware address, machine name, asset owner, department, and whether currently supported.
- Software asset inventory: Inventory, track, and maintain a detailed list of all software in use by the Town (OS and applications). Details to track should include application name, publisher/vendor, version, application owner, supporting database (if applicable), and if possible, whether software is currently up-to-date with latest patches.
- Configuration settings: (This is not exhaustive). Reliable baseline configurations in place. Administrative accounts should be dedicated, there should be a firewall implemented with rulesets configured appropriately, end-user devices should have a firewall enabled, default/vendor accounts should be locked down/prevented from use, unnecessary services/extensions/applications should be disabled; insecure ports should be blocked, password policy should meet current standards, lockout policy should be in place, MDM should be in place with remote wipe capabilities (only applicable if employees can access town data on mobile devices).
- Vulnerability scanning: Ideally, a continuous vulnerability solution is best, but dedicated vulnerability scans (internal and external) should be taking place at least once a year. AV/AM.
- Pentesting: The town should have an internal and external pentest at least once a year, performed by an external firm.
- Logs: Document which logs are being maintained (sys logs, audit logs, etc.), if any, and whether they are being reviewed actively or passively with any frequency. Ensure log configurations

cannot be modified. Ensure logs are stored securely and cannot be altered. This becomes important in the event of any forensic analysis needed following a breach.

- Access control: Make sure there's a consistent process to provision, change access, and deprovision access rights.
- Access review: Ensure that accounts (network, application) including administrative accounts are reviewed at least annually. Incorporate a policy to automatically deprovision/disable accounts that have not been logged into for 90 days.
- Backups: Establish and document a backup/recovery process, ensure backups are automated where possible and that they are isolated and adequately protected, test data recovery capabilities at least annually.
- Remote connections: Ensure secure connection via VPN (or other secure method). Avoid split-tunneling.
- IDS/IPS: Deploy if possible/affordable.
- Training: Security awareness training for all employees, including training on any applicable laws/regulations that apply to job responsibilities when dealing with data on citizens of the Commonwealth. Phishing and social engineering training. Role-based training, particularly for those in higher risk positions.
- Service Providers/Vendors: Maintain inventory of all 3rd party service providers/vendors, document process for vendor due diligence/vetting, ensure contracts include security language to adequately protect the Town's assets, have program in place to monitor providers or establish a requirement for regular status reports from vendors. Establish a process for "decommissioning" service providers.
- Incident handling: Ensure process is in place, key roles & responsibilities are assigned. Perform an incident response test at least annually.
- Pentesting: Engage an external party to perform a pentest at least annually, internal and external.
- Risk mitigation: Document all vulnerabilities and risks identified in a risk register and track milestones for remediation.
- Risk assessment: Perform internal risk assessment at least annually. Report findings to the BoS. Add findings to the Risk Register. Consider hiring an external to perform the risk assessment once every few years (if every year is not affordable).

Kind Regards,
Anna