Simsbury Technology Task Force
Regular Meeting
April 5, 2021 – 5:30pm

Watch this meeting LIVE on Comcast Channels 95, 1070, Frontier Channel 6070 and LIVE streamed or on-demand at www.simsburytv.org

Pledge of Allegiance

1. Approval of Minutes
    a. March 1, 2021

2. IT Policies Review
    a. Remote Access Policy

3. Next Steps/Agenda items for next meeting

Adjourn

Town of Simsbury

933 HOPMEADOW STREET SIMSBURY, CONNECTICUT 06070

Technology Task Force
Monday, March 1, 2021, 5:30 p.m.
Zoom Conference & SCTV Live Stream

Regular Meeting Minutes - DRAFT

Members Present: Harald Bender, Paul Kelley, Bill Rucci, John Jahne, Liz Peterson, Mike Doyle
Liaisons Present: Wendy Mackstutis (Board of Selectmen)
Staff Present: Rick Bazzano, Jason Casey, Melissa Appleby

The meeting was called to order at 5:34 pm by vice chair Paul Kelley. All stood for the pledge of allegiance.

1) **Minutes**
   a. **February 22, 2021 (Special Meeting)**
   b. **February 1, 2021 (Regular Meeting)**
   c. **January 28, 2021 (Special Meeting)**
   d. **November 30, 2020 (Special Meeting)**
   e. **November 12, 2020 (Special Meeting)**
   f. **October 21, 2020 (Special Meeting)**

   Mr. Bender noted that on the February 1, 2021 minutes, under section 3, the words "two" and "or" should be separated.

   Mr. Doyle made a motion to approve the minutes as presented, with the one noted change to the February 1 minutes. Mr. Bender seconded the motion. All were in favor and the motion passed unanimously.

2) **Shared Services Study**
   Mr. Rucci said that the subgroup believes that one document could represent the various shared services between the Town and Board of Education. He said that the final document covers governance, finance arrangements, and shared platforms. This will be signed by IT staff and reviewed on a regular basis. Mr. Kelley thanked Mr. Casey and Mr. Bazzano for their efforts. Mr. Bender noted that this summarizes the arrangement well, and it will allow the arrangement to survive any transitions in staff. Staff will report back to the Town Manager and Superintendent with the final version. Ms. Mackstutis requested that the final document be shared with the Board of Selectmen.

3) **IT Policies Review**
   a. **Acceptable Use Policy**
      Mr. Rucci reminded the group that it will begin reviewing all IT-related policies on an annual basis, starting with the two oldest. Mr. Bender suggested "including but not

limited to" to the fourth bullet point in the section titled "Prohibited Activities." The group discussed the meaning of "unusual occurrences," as referenced on page 3. Mr. Bazzano clarified that this is intended to instruct employees on what to do if anything out of the ordinary takes place with their technology. Ms. Mackstutis asked for confirmation that employees sign off on this policy; staff confirmed that they do.

Mr. Jahne made a motion to approve the proposed edit to the Acceptable Use Policy. Mr. Bender seconded the motion. All were in favor and the motion passed unanimously.

b. Incident Response Procedure

The group discussed possible wording changes to the document, including replaceing references to "School Business Manager" to "Assistance Superintendent for Administration." In several sections, the lists will be updated to remove semi-colons and make other clean-up changes. There was some discussion regarding the addition of "including but not limited to" to several sections. Mr. Rucci reminded staff that the list of external contacts should continue to be maintained separate from this document.

Ms. Mackstutis suggested adding guidance for when the Board of Selectmen and Board of Education should be notified of an incident. Ms. Appleby informed the group that the public safety sub-committee is planning to hold a tabletop exercise on cyber security, and further revisions to this document are likely forthcoming. Discussion ensued regarding the value of a tabletop exercise. Mr. Doyle reminded the group that this document provides a framework, and a tabletop exercise will test all of the areas covered in it.

The group decided not to formalize any recommended changes to the document until the tabletop exercise has taken place.

4) Next Steps/Agenda items for next meeting

There was brief discussion on the security system at Simsbury High School. Mr. Casey said that the individual in the new security position is managing this project. There was consensus that although this project includes a technology component, it is focused more on physical security.

For the next meeting, the group will review the Remote Access Policy.

Mr. Rucci made a motion to adjourn the meeting at 6:29 pm. Mr. Doyle seconded the motion. All were in favor and the motion passed unanimously.

Respectfully Submitted,
Melissa Appleby
Deputy Town Manager

Town of Simsbury

933 HOPMEADOW STREET ~ SIMSBURY, CONNECTICUT 06070

TOWN OF SIMSBURY
Remote Access Policy
Adopted by the Board of Selectmen on January 28, 2019

Purpose
This policy defines objectives, responsibilities and requirements for securing remote user access using Virtual Private Network (VPN) and other technologies to connect to the Town of Simsbury internal network and information systems.

Remote access is for the sole convenience of the Town of Simsbury and shall not be construed as conferring any independent rights upon the individual or firm granted such access through this Policy. Remote access rights may be cancelled at any time by the Town Manager or his/her designee for any reason or for no reason in his/her sole discretion.

Scope
This policy applies to all Town employees, consultants, third party vendors and others that are granted access to Simsbury's network and information systems. This policy applies to all remote access used to conduct Town business.

Definitions
Virtual Private Network (VPN): technology used to extend Simsbury's private network across the internet. VPNs only provide secure access into Simsbury's network. VPNs do not provide Internet connectivity. Examples of VPNs include firewall-based VPN client software, Virtual desktops, and Web-based remote access services such as Webex, Logmein and Bomgar.

Requirements
- Secure remote access is strictly for authorized employees, vendors, contractors and agents of the Town of Simsbury. Anyone authorized for remote access must not at any time allow any unauthorized individuals to use their connection, share their password, or provide other information needed to gain access to the town of Simsbury networks.
- Only those remote access clients and operating systems approved by the Simsbury Information Technology (IT) Department are permitted. All clients will be configured to meet approved standards and requirements for authentication, encryption and auditing. The IT department will maintain a list of approved users; the list is not under change control for this document and will be maintained separately.
- All connections to the Town of Simsbury networks and information systems will be logged and monitored.
- Remote access users are responsible for acquiring and using their own Internet service to access the Town's networks.

- At no time will the Town of Simsbury be responsible for covering any costs associated with acquiring or using personal internet services or devices.
- VPN accounts for authorized users will only be created at the request of the user's department head or division director who must submit a signed request to the Town Manager. VPN accounts will be created on an individual basis, secured with assigned credentials, including a username and password. Shared accounts are not permitted. Every remote access user must have a unique set of credentials.
- Remote access clients will only be installed on Town of Simsbury issued laptops or other equipment as directed by the IT Manager. The Town will not provide support for remote access clients installed on vendors' or individual users' personal devices.
- Vendors with remote access credentials will comply with security controls as specified in their written agreement or contract with the Town of Simsbury, including the privacy disclosure statement.
- Modifying or reconfiguring the remote access clients, the computer, its operating system or other network equipment for the purpose of bypassing required security controls is not permitted at any time.
- All devices (such as computers, laptops, servers, wireless access points and mobile phones) that are connected to the Town networks via remote access technologies must use the most up-to-date end point protection (firewall, malware and anti-virus services), current operating system patches and manufacturer supported operating systems.
- Remote connections will be configured to enforce inactivity timeouts.
- Use of the Town's remote access technology constitutes consent to this policy.

Responsibilities
All users are responsible for familiarizing and complying with the Remote Access Policy. The Town of Simsbury's IT staff is responsible for deploying and maintaining software and technologies in support of this policy.

Enforcement
Employees that are found to have violated this policy may be subject to discipline up to and including termination without lower levels of discipline having been issued depending on the nature and severity of the offense or offenses. Any discipline issued shall be in accordance with procedures outlined in the employees' relevant collective bargaining agreements or the Town Personnel Rules as applicable.

Third-party vendors that are found to have violated this policy may be subject to a termination of their contract with the Town.

In addition, disclosure to law enforcement agencies may be required for violations of applicable laws and regulations.

IT Policies

POLICY	ADOPTED	REVISED	SUMMARY	ENTITY
Acceptable Use Policy	10/11/2017	11/27/2017	Outlines the acceptable use of Town technology resources (email, internet, printing, mobile devices, file storage, telephone systems, etc.).	Town
Remote Access Policy	1/28/2019		Defines objectives, responsibilities and requirements for securing remote user access using VPN and other technologies to connect to the Town of Simsbury internal network and information systems.	Town
Social Media and Website Use Policy	3/11/2019		Provides standards and procedures for the establishment and appropriate use of social media and website accounts.	Town
Incident Response Procedure	5/15/2018		Clarifies roles and responsibilities in the event of a serious cyber incident and establishes a procedure for responding to serious cyber threats to the organization.	Town/BOE
Technology Task Force Procedures Policy	11/9/2020		Outlines the purpose of the Task Force, membership composition, and operational procedures for the committee.	Town/BOE