Simsbury Technology Task Force
Regular Meeting
March 1, 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. 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)

2. Shared Services Study

3. IT Policies Review
    a. Acceptable Use Policy
    b. Incident Response Procedure

4. Next Steps/Agenda items for next meeting

Adjourn

Technology Task Force
IT Shared Services Sub-Group
Monday February 22, 2021, 2:00 p.m.
Zoom Conference & SCTV Live Stream
Special Meeting Minutes – Draft

Members Present: Harald Bender, Paul Kelley, Bill Rucci, John Jahne

Staff Present: Rick Bazzano, Jason Casey

The meeting was called to order at 2:00 p.m. by sub-group chair Bill Rucci.

Shared Services Study – Draft MOU – Sharing of IT Services

Mr. Rucci opened the meeting, thanking attendees for their time, and specifically thanking Jason Casey and Rick Bazzano for their work in refining the draft Sharing of IT Services MOU. Using the updated MOU as our guide, Mr. Bazzano walked the group through the most recent changes and areas of focus.

Meeting attendees had several questions and comments, and these were discussed for possible inclusion in the finalized version.

Consideration will be given to adding bullet points (associated with IT Steering) regarding the “sharing & agreement on IT priorities”, as well as “resolving any IT related issues”. And, the section under Financial Agreement will be adjusted slightly based on the discussion. Like other IT policies, this MOU will be reviewed on a regularly scheduled basis, for future update and continued value.

Next Steps/Agenda items for next meeting

Mr. Bazzano and Mr. Casey agreed to update the Sharing of IT Services MOU with the input from today’s meeting.

Mr. Bender made a motion to adjourn the meeting at 2:20 p.m. Mr. Kelley seconded the motion.

.
Respectfully Submitted,
Bill Rucci

Town of Simsbury

933 HOPMEADOW STREET SIMSBURY, CONNECTICUT 06070

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

Regular Meeting Minutes - Draft

Members Present: Harald Bender, Paul Kelley, Ray Rosati, Bill Rucci, John Jahne, Liz Peterson, Evan Marks
Liaisons Present: Wendy Mackstutis (Board of Selectmen), Brian Watson (Board of Education)
Staff Present: Rick Bazzano, Jason Casey, Melissa Appleby

The meeting was called to order at 5:30 pm by chair Evan Marks. All stood for the pledge of allegiance.

1) **Minutes**
   Mr. Bender made a motion to approve the minutes of December 7, 2020. Mr. Rosati seconded the motion. All were in favor and the motion passed unanimously.

2) **Shared Services Study**
   Mr. Rucci updated the group on the special meeting held by the subgroup on January 28. He said there were good examples to work from provided by Mr. Marks, and Mr. Casey put together a draft. Mr. Casey and Mr. Bazzano will take the feedback from the subgroup and revise the draft; then the subgroup will meet again in February. The full Task Force will review the document in March.

3) **IT Policies Review**
   Mr. Marks directed the group to the list of policies, and asked for feedback on a review schedule. Mr. Rosati asked whether a twoor three-year review cycle would be appropriate; Mr. Jahne shared that his company does annual reviews. The group decided to review annually, starting with the two oldest policies (Acceptable Use and Incident Response Procedure). From there, one policy will be reviewed each quarter. Ms. Appleby will make sure all policies are saved to the group's Google Drive.

4) **Next Steps/Agenda items for next meeting**
   The group will review the draft shared services document and the two noted policies at the next meeting.

Mr. Bender made a motion to adjourn the meeting at 5:45 pm. Mr. Jahne seconded the motion. All were in favor and the motion passed unanimously.

Respectfully Submitted,
Melissa Appleby
Deputy Town Manager

Technology Task Force
IT Shared Services Sub-Group
Thursday, January 28, 2021, 10:00 a.m.
Zoom Conference & SCTV Live Stream
Special Meeting Minutes – Draft

Members Present: Harald Bender, Paul Kelley, Bill Rucci, John Jahne

Staff Present: Rick Bazzano, Jason Casey

The meeting was called to order at 10:00 a.m. by sub-group chair Bill Rucci.

Shared Services Study – Document Areas of IT Sharing

Mr. Rucci acknowledged the fact that the group had received several examples of MOU documents (from Mr. Evan Marks) and that Mr. Jason Casey had developed a draft MOU document titled Sharing of IT Network Services. This document was used as a basis for discussion and Mr. Casey walked the group though it in detail, as the sub-group members offered suggestions and asked questions.

The meeting attendees agreed that this document should be expanded to cover (at a high level) all areas of IT sharing and Governance for Simsbury. This will reduce the need for individual documents for shared platforms, services and staff, as well as highlighting how IT Governance (IT Steering Committee) guides IT direction. Taking this approach should make regular updating of the MOU (s) more efficient and still provide needed insights/direction as to the criticality/benefits of IT sharing.

Next Steps/Agenda items for next meeting

The sub-group requested that Mr. Casey and Mr. Bazzano update the IT Sharing MOU with the input from today's meeting. We will review the updated document at a future sub-group meeting.

Mr. Kelley made a motion to adjourn the meeting at 10:50 a.m.. Mr. Bender seconded the motion.

.
Respectfully Submitted,
Bill Rucci

Town of Simsbury

933 HOPMEADOW STREET SIMSBURY, CONNECTICUT 06070

Technology Task Force
Shared Services Subgroup
November 30, 2020 – 3:30pm

Special Meeting Minutes - Draft

Members Present: Bill Rucci, Harald Bender, Paul Kelly

Staff Present: Melissa Appleby, Rick Bazzano

The meeting was called to order at 3:30pm.

1) Shared Services Study Discussion
The group reviewed the sample MOUs from Mansfield and Enfield, and compared the two arrangements in regards to governance, budgeting, and personnel management. Mr. Bazzano provided a detailed overview of how the current shared services arrangement between the Town and Board of Education compares with these more formal arrangements. Some of the areas that we currently share, or partially share, include: network infrastructure, network security, fiber, internet connection, financial database/software, IT steering committee. Some areas that are separate include: phone systems, email, help desks.

Discussion ensued regarding whether we should formalize these arrangements or consider consolidation between the Town and BOE. After some discussion, the group determined that we are already collaborating and sharing in ways that are similar to towns that have more formal shared services arrangements, and that there is value in documenting and formalizing those arrangements.

Adjourn
The meeting adjourned at 4:25pm.

Respectfully Submitted,
Melissa Appleby
Deputy Town Manager

Town of Simsbury

933 HOPMEADOW STREET SIMSBURY, CONNECTICUT 06070

Technology Task Force
Shared Services Subgroup
November 12, 2020 – 3:30pm

Special Meeting Minutes - Draft

Members Present: Bill Rucci, Harald Bender, Paul Kelly

Staff Present: Melissa Appleby, Rick Bazzano

The meeting was called to order at 3:30pm.

1) Shared Services Study Discussion
Staff gave an oral report on the lessons learned from four municipalities that have shared services between the Town and Board of Education – Mansfield, West Hartford, Enfield and Suffield. A few takeaways include: leadership on the Town and Board of Education must be on the same page and interested in collaborating; each model is structured slightly differently in regards to the reporting structure, method of budgeting, etc.; a separate curriculum/instructional technology director is still required on the Board of Education side.

Discussion ensued regarding the governance structure under these models, and the importance of setting up a formal arrangement that determines how priorities are set and how decisions are made. The group also discussed the importance of determining the scope of services, and defining whether it will cover infrastructure, applications, or both.

There was consensus that we should document our existing shared services. The group agreed to review the sample MOUs from other towns and begin framing out the key components of a governance structure.

Adjourn
The meeting adjourned at 4:15pm.

Respectfully Submitted,
Melissa Appleby
Deputy Town Manager

Town of Simsbury

933 HOPMEADOW STREET SIMSBURY, CONNECTICUT 06070

Technology Task Force
Rules of Procedure Subgroup
October 21, 2020 – 12:30pm

Special Meeting Minutes - Draft

Members Present: Mike Doyle, Ray Rosati, John Jahne, Liz Peterson

Staff Present: Melissa Appleby, Rick Bazzano

The meeting was called to order at 12:31pm by Mike Doyle.

1) Rules of Procedure Discussion
The group reviewed the draft prepared by staff, and discussed the following sections in detail:

- Purpose – The group created a mission statement several years ago; this langyage will be used in this section
- Composition – The group agreed that nine members is appropriate
- Meetings – The group agreed to continue with monthly meetings, and to include language to allow for subgroups to meet as needed
- Reports – There was discussion around the need to more formally document the recommendations that the committee provides to IT staff, as this can help lay the groundwork for future presentations to the Board of Selectmen. The group decided that having the annual report to the Board occur in November makes sense, as new terms begin in December

Ms. Appleby will circulate the draft to the full Task Force for review in advance of the next regularly scheduled meeting.

Adjourn
The meeting adjourned at 1:18pm.

Respectfully Submitted,
Melissa Appleby
Deputy Town Manager

Final 2/27/21

MEMORANDUM OF UNDERSTANDING

Sharing of IT Services

The Simsbury Public Schools IT Department

and

The Town of Simsbury IT Department

This agreement made and entered into this _____ day of _____, 2021 by and between the Town of Simsbury (hereinafter referred to as the "Town") and the Simsbury Board of Education (hereinafter referred to as the "BOE"), collectively referred to as the "Parties."

Goal, History, and Purpose

It is the goal of the BOE and the Town to continually look for areas of increased cooperative efforts that benefit both organizations and provide efficiency.

The IT Departments of Simsbury Public Schools and the Town of Simsbury have a strong history of sharing resources. To date, this has been accomplished informally.

The purpose of this Memorandum is to formalize the relationship between the two IT departments by documenting the existing areas of collaboration along with the expectations of responsibility that have evolved over time.

Rationale and Specific Understandings

1. Representatives of the Town and BOE will meet regularly to discuss the technology related goals, initiatives, and projects of both parties. The purpose of these meetings will be to:
    - ensure collaboration of expertise and experience with an understanding on priority areas of technology within each department,
    - open discussions and resolve on major IT issues that may arise,
    - explore opportunities for efficiencies of scale through combined efforts, and
    - prevent inefficient duplicative use of resources.
    - review and revise policy and procedural documents, such as this MOU

    These meetings will be accomplished through attendance in the following groups:
    - The IT Steering Committee
        - Town Membership: Deputy Town Manager, IT Manager
        - BOE Membership: Director of Infrastructure & Technology
    - The IT Task Force
        - Town Membership: Deputy Town Manager, IT Manager, BOS Liaison, Citizen Members

- BOE Membership: Director of Infrastructure & Technology, BOE Liaison

2. The IT departments of both parties will manage, and maintain the Microsoft AD Domain Controllers in their respective server rooms. Any decisions or actions that may impact AD performance will be discussed amongst the administrators of those two departments prior to taking place.

3. The IT departments of both parties will share knowledge of any significant security threats to either organization per the documented "Incident Response Policy".

4. The BOE will freely provide colocation space in the server room located at Simsbury High School to the Town for the purpose of running redundant networking equipment. This will include the use of available rack space, UPS protected power, and network connectivity.

5. The BOE will freely provide a 100Mbps Internet connection to the Town's Public Library for the duration of the BOE's contract with the Connecticut Education Network (CEN). This connection will be made behind the BOE's firewall. The BOE makes no guarantee, expressed or implied, for the safety of this connection.

6. The BOE will continue to manage, and maintain the "HSMail" Microsoft Exchange server until July 1st, 2022. This Email server, located at Simsbury High School, was initially used to provide Email service to both parties. It is currently used by the BOE to forward messages sent to their old domain name, and by the Town as an Email proxy server. Both of these needs should expire by July 1st, 2022.

7. The BOE will continue to manage and maintain the Barracuda Email archive appliance. This appliance, located at Simsbury High School, was initially used to archive both BOE and Town Email. The BOE uses a different Email archive solution at this time, but maintains the appliance for its store of old BOE Email, and its ongoing archival operation of Town Email.

8. The BOE will continue to provide, manage, and maintain its own Aruba WIFI equipment in the BOE offices located at Simsbury Town Hall. Access to the BOE's public WIFI will be available to anyone within range at that location.

9. The BOE and the Town will continue to freely share use of the fiber optic, wide-area network cables installed by both organizations.

10. The Town will manage, maintain, and provide implementation assistance with the KnowBe4 anti-phishing training program. The cost of this program will be split evenly by the Town and BOE.

11. The Town will freely include BOE targets in the configuration of the quarterly network penetration testing it contracts for through CI Security. The Town will freely share the results of that testing with the BOE when it is completed.

12. The Town will continue to manage, maintain, and support the shared financial software (Finance Plus, Munis, etc) used by both parties.

13. The Town will continue to assist the BOE in managing the integration of the BOE's Employee Access Center (EAC) software with the shared financial software.

Financial Understanding

Simsbury Public Schools will contribute 50% of the salary and benefits of the Town of Simsbury IT Manager and IT Analyst annually through the School Business Office as per the 2020 MOU for shared services.

Simsbury Public Schools will contribute 50% of the cost of the KnowBe4 anti-phishing training program, purchased by the Town.

The Town of Simsbury will provide, maintain, support, and manage the computer equipment needed for the normal business operation of the Board of Education offices located within Simsbury Town Hall at 933 Hopmeadow St., and the office of the BOE's Director of Operations, located within the Town Garage facility at 66 Town Forest Rd. This equipment includes, but is not limited to desktop computers, laptops, printers, projectors, and network infrastructure.

The parties also agree to maintain regular and open communication to evaluate the effectiveness of this agreement and suggest improvements and adjustments that may be necessary.

Duration

This agreement shall remain in effect until such as the agreement is modified or terminated by the consent of the parties. It may be modified at any time by amendment to the agreement.

SIMSBURY PUBLIC SCHOOLS

_____

Jason Casey, Director of Infrastructure & Technology

TOWN OF SIMSBURY

_____

Rick Bazzano, IT Manager

Latest Document review and/or update – February 22, 2021

TOWN OF SIMSBURY
ACCEPTABLE USE POLICY

Overview

The Town of Simsbury (the "Town") provides Town employees and, on occasion, members of boards, committees and commissions, contractors, consultants and temporary employees (the "Users") with technology and communications resources which are intended to facilitate official business of the Town. All use of such resources shall be conducted in an honest, ethical, and legal manner that conforms to applicable license agreements, contracts and policies regarding their intended use. The IT Department is responsible for protecting both employees and the Town from illegal or damaging actions by individuals, either knowingly or unknowingly.

Purpose

The purpose of this policy is to outline the acceptable use of the technology and communications resources available to Users. These resources include but are not limited to computing, electronic communications, printing, mobile devices, file storage and telephone systems. This policy is in place to protect both Users and the Town. Inappropriate use exposes the Town to risks that could lead to loss or misuse of data and systems resulting in substantial costs or potential legal issues.

All systems, communications and stored information transmitted, received or contained in those systems are the property of the Town. All Users are responsible for exercising good judgment regarding the use of technology and information in accordance with Town policies and standards, and federal and local laws and regulations.

Policy

Security of Town Information

Town information, regardless of where it is stored, is the property of the Town. Users may access, use or share Town information only to the extent it is authorized and necessary to fulfill assigned job duties. Users have a responsibility to immediately report the theft, loss or unauthorized disclosure of Town information to the Technology Manager.

Town information, including e-mail, is public record, and retention and disposition of those records are authorized by retention schedules issued by the State of Connecticut. Town departments may retain downloaded files in hard copy, electronically, or by a combination of these two means. Town departments are responsible for developing filing systems that include downloaded files and are responsible for instructing employees on appropriate use of these systems.

Access to Internal Network

All mobile and computing devices that connect to the internal network must comply with the minimums stated in Simsbury's Access Policy.

System level and user level passwords must comply with the Simsbury Access Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. All computing devices must be secured with a password-protected screensaver with

the automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.

Downloading or Opening Files

Users must use extreme caution when clicking links, downloading files or opening email attachments from any party, including known senders, as they may contain malicious or illegal content. Users who question the intent of links, files or attachments from known senders should verify intent through other means of communication prior to opening.

Procedures

1. ***Electronic Mail:*** The e-mail system should only be used for Town business. The Town reserves the right to monitor all electronic mail communications to ensure that they are being used in accordance with this policy. As noted above, e-mails are public records and are subject to State and Federal disclosure laws and record retention requirements (CGS Chapter 14, Sec. 1-211).

2. ***Internet Access:*** To the extent that Users are given access to the internet to facilitate the conduct of Town business, Users have the responsibility to use these resources in accordance with State and Federal Law. Users may only access the internet through the Town-owned firewall. The Town uses internet content filtering and usage monitoring technology. Monitoring includes but is not limited to websites accessed and the amount of time spent by any User on a web site.

3. ***Social Media:*** "Social media" includes all means of communicating or posting information on the internet, including but not limited to blogs, personal websites, social networking or affinity websites, web bulletin boards or chat rooms.

   Use of social media from the Town's systems is subject to monitoring. Limited and occasional use of the Town's systems for social media purposes is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the Town's policies, is not detrimental to the Town's best interests, and does not interfere with a User's regular work duties.

   Town e-mail addresses may not be used for social networks, blogs, or other online tools for personal use. The Town's intellectual property may not be used in connection with any social media activity.

   Before creating online content, Users should consider their responsibilities to the Town. Confidentiality of private and proprietary information, including protected health information, must be maintained. Users must express only their own opinions and make clear that their views do not represent the views of the Town.

Appropriate Use

Internet use on Town resources shall be for business matters directly related to the operational activities of the Town. Users are responsible for exercising good judgment regarding the

reasonableness of personal use. Incidental personal use of the computer systems may be permitted solely for the purpose of e-mail transmissions and access to the internet on a limited, occasional basis. Such incidental personal use of the computer systems shall not interfere in any manner with work responsibilities, and is subject to all rules, including monitoring of all such use.

Prohibited Activities

The following activities are strictly prohibited:

- Activities that could cause congestion and disruption of networks and systems, including but not limited to consuming excessive system resources, e.g. music or video streaming.
- Solicitation or proselytizing for commercial ventures, religious, or political causes, outside organizations, or other non-job related solicitations.
- Downloading of any software or programs from the internet without the prior express permission of the Technology Manager.
- Unlawful activities, threats, harassment, slander, defamation or gambling.
- Accessing, downloading or storing any materials that promote discrimination on the basis of race, color, national origin, age, marital status, sex, political affiliation, religion, disability, gender identification or sexual preference.
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Town.
- Revealing your account password to others or allowing use of your account by others.
- Accessing adult content, including but not limited to sexually explicit material.

Unusual Occurrences

All matters relating to unusual occurrences must be reported immediately to the Technology Manager. When something unusual occurs, Users are advised to record information such as steps taken and warnings from the computer. This will aid the Technology Department in diagnosing the situation.

Monitoring and Compliance

Use of the Town's technology and communications resources constitutes consent to monitoring of usage activity and is conditioned upon strict adherence to this policy. Users should not have any expectation of privacy regarding any items stored or transmitted via the Town's information technology resources. The First Selectman/Selectwoman or Town Manager reserves the right to audit network activity and internet access on a periodic basis to ensure compliance with this policy. Any employee who violates this policy shall be subject to disciplinary action and possible loss or suspension of associated IT privileges.

Approved by the Board of Selectmen on November 27, 2017

Cyber Incident Response Procedure
Town of Simsbury and Simsbury Board of Education

Purpose

This written plan is enacted to clarify roles and responsibilities in the event of a serious cyber incident and to establish a procedure for responding to serious cyber threats to the organization. The availability of cyber resources is critical to the operation of the organizations and a swift and complete response to any incidents is necessary in order to maintain that availability and to protect information.

Incident Response Team

Responsible Executive Officer (REO)

If the incident affects the Town of Simsbury, the Town Manager shall be the Responsible Executive Officer. If the incident affects the Board of Education, the Superintendent of Schools shall be the Responsible Executive Officer. If both organizations are affected, the Town Manager and the Superintendent of Schools will serve as joint REOs.

The REO oversees the entire response process, manages the overall response activities for all security incidents, makes decisions regarding which courses of action will be taken and determines when it is appropriate to share information outside the organization. The responsibilities of the REO include, but are not limited to:

- Receiving initial notification and status reports from the Incident Response Manager;
- Consulting with the Town's Public Information Officer on public notification and assisting with the preparation of press releases and other communications as needed;
- Consulting with Legal Counsel;
- Consulting with internal staff on priorities for response and recovery; and
- Advising the Incident Response Manager on priorities.

Incident Response Manager (IRM)

The Town of Simsbury designates the Deputy Town Manager, and the Simsbury Board of Education designates the Business Manager, as their respective Incident Response Managers. The IRM has the overall responsibility to ensure the implementation, enhancement, monitoring and enforcement of security policies and procedures. This person shall understand incident handling, be familiar with the organization's network and systems, and is responsible for preparing for and coordinating the response to a serious cyber incident. Responsibilities include, but are not limited to:

- Developing and testing response plans;
- Coordinating incident response;
- Involving the identified technical support to address a serious incident;
- Notifying the appropriate executive that a serious incident has occurred;
- Notification of law enforcement (including local, state and federal organizations) and Legal Counsel as appropriate when a serious incident has occurred;

- Advising the REO and peer Town or Board of Education IRM regarding notification of law enforcement and Legal Counsel if appropriate;
- Providing information to the Public information Officer for notifying the press and public;
- Coordinating the logging and documentation of the serious incident and the response to it; and
- Making recommendations to reduce exposure to the same or similar incidents in the future.

Information Security Officer (ISO)

The Information Security Officer shall be the IT Manager designated by the Town of Simsbury and the Simsbury Board of Education respectively. The ISO shall be responsible for the security of day-to-day technology operations and shall serve as the initial point of contact for cyber security concerns. Specific responsibilities under this plan include:

- Serving as the initial point of contact for technology users who are concerned that a cyber incident may have occurred;
- Making an initial determination with respect to any concerns presented;
- Alerting the Incident Response Manager and peer ISO in the event of a potentially serious breach of security;
- Overseeing the Technical Support Staff response to a security breach;
- Consulting with internal staff on priorities for response and recovery;
- Maintaining and updating annually a list of internal and external contacts (attached hereto as Appendix A, which is not under change control for this document), including but not limited to:
    - Insurance contact for reporting a security breach;
    - MS-ISAC, CCAT and other potential sources for technical support;
    - Critical hardware and software vendors;
    - Law enforcement reporting contacts (including but not limited to the Connecticut Intelligence Center); and
- Regularly updating the IRM of the status of the organization's response to a security breach.

Public Information Officer

The individual (as identified by the Town of Simsbury and the Board of Education respectively) primarily responsible for communication with the public in emergency situations.

Technical Support Staff

The IT organizations for the Town of Simsbury and the Simsbury Board of Education respectively shall provide technical support to the Incident Response Manager and the Information Security Officer. Responsibilities include, but are not limited to:

- Assessing the situation and providing corrective recommendations to the ISO and the IRM;
- Helping the ISO with the initial response to incidents;
- Responding to the incident to contain and correct problems;
- Reporting to the Incident Response Manager on actions taken and progress; and
- Participating in review of the incident and development of recommendations to reduce future exposure.

Legal Counsel

The Town of Simsbury's appointed legal counsel shall provide advice as called upon.

Incident Response Procedure

The Incident Response Procedure includes the following steps and responsibility for each step:

- Identification of a security breach (all end users)
- Determination of the existence of a serious security incident using the Threat Assessment Guide attached as Appendix C (ISO and IRM). As set forth in the Threat Assessment Guide, a serious security breach (a "serious incident") is generally defined as Threat Level 2 or greater and should at a minimum be reported to the peer ISO and IRM. Whether or not a "serious incident" will trigger activation of the Incident Response Procedure depends upon the nature and scope of the threat as determined by the ISO/IRM. Incidents defined as Threat Level 3 will generally trigger full activation of the Incident Response Procedure.
- Implementation of a response to the incident (ISO and Technical Support Staff)
- Documentation of the incident, including collection of evidence as necessary, and preparation of a report on the incident (Technical Support Staff, ISO and IRM)
- Technical repair of the affected technology infrastructure (ISO, Technical Support Staff, external resources as necessary)
- Communication concerning the incident both inside and outside the organization, including but not limited to press releases, communication with vendors, reports to law enforcement, etc. (REO, IRM, Legal Counsel)
- Determination of additional steps necessary above and beyond technological repair (such as notice with reporting requirements, compliance with the law, possible legal action against the intruder, etc.). (REO, IRM, Legal Counsel)
- Review the overall effectiveness of the response procedures (REO, IRM, ISO, Technical Support Staff, others)
- Evaluate whether changes to existing security or new security measures are necessary; implement as needed (REO, IRM, ISO, Technical Support Staff).

1. **Identification of a Security Breach**

    a. Users of technology shall be trained to recognize potential security breaches and instructed to immediately report any signs of anomalous activity to the ISO. Training shall be conducted on a periodic basis and shall be designed to help users recognize and avoid potential cyber security threats as well as report any such threats to the ISO.

    Possible Causes
    Possible causes of cyber incidents include the following:

    - Attempts to gain unauthorized access to a system or its data
    - Unwanted disruption or denial of service (DoS)
    - Unauthorized access to critical computers, servers, routers, firewalls, etc.
    - Changes to system hardware or software without approval
    - Virus or worm infection, spyware, malware and ransomware

- Loss of, or inconsistent, electrical power

Symptoms

Signs a computer has been compromised may include the following:

- Abnormal response time or non-responsiveness
- Unfamiliar or suspicious pop-up screens
- Unexplained account lockouts
- Passwords not working
- Website homepage won't open or has unexplained changes/content
- Programs not running properly
- Running unexpected programs
- Lack of disk space or memory
- Bounced-back emails
- Inability to connect to the network
- Constant or increasing crashes
- Abnormal hard drive activity
- Connecting to unfamiliar or undirected websites
- Browser settings changed
- Extra toolbars that cannot be deleted

This list is not comprehensive, but is intended to raise the level of awareness of potential signs. If an employee is unsure about a possible incident, he/she shall treat the incident as a security event and notify the ISO who will work with the organization's Technical Support Staff.

2. **Threat Assessment**

a. In addition to regularly monitoring the security of the organization's technology, the ISO shall review all reports of suspicious activity and determine (1) whether or not a security breach has occurred, and (2) if so, the degree of threat presented by the breach using the Threat Assessment Guide attached hereto as Appendix C. If the breach presents a low-level threat which can be easily eliminated, the ISO shall work with Technical Support Staff to eliminate the threat. If the incident appears to be a "serious incident," as defined herein, which threatens the confidentiality, integrity or availability of the organization's information resources, the ISO shall contact the IRM within a 24-hour period who may initiate the Incident Response Procedure. Questions that should be addressed include: What are the symptoms? What may be the cause? What is being impacted? How widespread is it? What part of the system or network is impacted? Could this impact our constituents and/or associates?

3. **Implementation of the Incident Response Procedure**

a. **Documentation.** When the ISO and the IRM have determined that a serious incident presenting a significant threat has occurred, the IRM and ISO shall begin the process of recording information about the event in an Incident Log (attached as Appendix B). The following types of information shall be documented:

- Organization's name
- Characteristics of incident
- Date and time incident was detected, and name of person first detecting it
- List of symptoms identified
- Scope of impact
    - How widespread
    - Number and identity of users impacted
    - Number of machines affected
- Nature of incident
    - Denial of Service
    - Malicious code
    - Scans
    - Unauthorized access
    - Other (specify)

Incident logs shall be kept together in one location. This information is useful for information-sharing and incident reporting, and can be used to inform recommendations for reducing future exposure to similar incidents.

b. **Technical Repair.** The ISO shall determine the steps necessary to protect the confidentiality, integrity or availability of the organization's information resources and to repair any damage to the integrity of the organization's information infrastructure. The ISO shall work with the Technical Support Staff and shall bring in external resources as necessary to protect the organization and restore safe operations. Technical Support Staff shall first isolate the problem, which may mean disconnecting the equipment from the network or if no network exists, the Internet. Additionally, the Technical Support Staff shall examine the equipment and check the appropriate logs, such as the firewall and system logs for signs of unauthorized access. Performing a vulnerability scan is helpful to identify vulnerabilities that may have led to the incident. It may be necessary to bring in an outside expert to provide assistance.

c. **Communication.** As soon as practicable (within two hours), the IRM shall notify the REO of the incident. The IRM shall also confer with the REO, PIO, insurance representatives, law enforcement representatives and Legal Counsel to brief them on the situation. The briefing(s) shall include a discussion and determination whether or not communication, including communication to the public and/or communication to individuals or organizations affected by the incident, is warranted, recommended or legally required and if so, the content of the communication. The final decision with respect to communication rests with the REO. Unless the REO determines otherwise, the PIO shall be the sole contact for public inquiries about the incident.

d. **Additional Steps.** The IRM shall also confer with the REO, PIO, insurance representatives, law enforcement representatives and Legal Counsel to determine what additional steps, if any, should or must be taken (such as consideration of litigation options, provision of identity theft protection to affected individuals, recommended capital expenditures, etc.).

4. **Post-Incident Review**.

    a. **Report.** Once a serious incident has been contained and any additional steps have been approved, the IRM shall prepare a post-incident report documenting the actions taken and based on the incident log prepared during the event. The report shall include the following:

        - Dates and times when the serious incident was detected
        - List of symptoms
        - Scope of impact
        - Step-by-step actions
        - Plans to prevent incidents of a similar nature in the future

    b. **Review.** The REO shall conduct a debriefing to examine the effectiveness of the response procedures and determine any necessary changes in procedure. The debriefing should particularly focus on any remaining vulnerabilities faced by the organization. The REO shall determine what information from the debriefing will be shared.

Appendix A: Emergency Contact List
(names and contact information maintained separately)

TOWN PERSONNEL

- Town Manager
- Deputy Town Manager
- Town Technology Manager
- Town IT Analyst
- Simsbury Police Department
- Superintendent of Schools
- School Business Manager
- School Director of Systems Technology
- School Network Manager
- Town Legal Counsel

EXTERNAL CONTACTS

- CT Intelligence Center
- CIRMA
- MS-ISAC

Appendix B: Incident Log

Reported By:

- Name:
- Department/Location
- Phone:
- Email:

Date and Time of incident detection:

Nature of Incident:

- ☐ Denial of Service
- ☐ Malicious Code (worm, virus)
- ☐ Scans and Probes
- ☐ Ransomware
- ☐ Unauthorized Access
- ☐ Website Defacement
- ☐ Other

If Other, please describe:

Incident Description (What was the individual working on when this occurred, and what were the signs or symptoms?):

Details (e.g. virus name, events, etc.):

Course of Action:

Additional Notes:

Appendix C: Threat Assessment Guide

This Guide is provided to aid in determination of the existence of a serious security incident by the ISO and the IRM. A serious security breach (a "serious incident") is generally defined as Threat Level 2 or greater and should at a minimum be reported to the peer ISO and IRM. Whether or not a "serious incident" will trigger activation of the Incident Response Procedure depends upon the nature and scope of the threat as determined by the ISO/IRM. Incidents defined as Threat Level 3 will generally trigger full activation of the Incident Response Procedure.

Nature of Incident	Threat Level		
	1 - Minimal Impact	**2 - Moderate Impact**	**3 - Severe Impact**
Scans and Probes	Intruder is conducting general reconnaissance *Example: A student exploring and collecting network information*	Intruder is conducting targeted reconnaissance *Example: An employee seeking specific information they are not entitled to*	Intruder has gained access to sensitive data *Example: An intruder deploys keylogger software*
Unauthorized Access	Intruder gains limited access to non-sensitive data *Example: A user logs on with a similar user's credentials for a stated non-malicious intent*	Intruder gains wide access to non-sensitive data *Example: A server is breached but the content would be available through FOI request*	Intruder gains access to sensitive data *Example: An external hacker accesses health records or financial data or data that could potentially aid in the commission of a crime*
Denial of Service	The DoS target is non-critical and affects a small number of users *Example: A DoS attack on a teacher website*	The DoS target is non-critical but affects a significant number of users *Example: A DoS attack on the wifi of a building*	The DoS target is a critical system *Example: A DoS attack on a fiber link*
Malicious Code (worm virus)	A single user's device is infected with malicious code that somehow eludes or defeats our defenses *Example: A virus on a thumb drive impacts the performance of a PC*	Multiple devices are infected with malicious code that somehow eludes or defeats our defenses *Example: Several users click an emailed link that installs spyware*	The organization is at risk of infection from a specific known threat that can somehow elude or defeat our defenses *Example: A user clicks a Facebook link that triggers a new worm on our network*
Ransomware	N/A	One or more devices are infected with ransomware that somehow eludes or defeats our defenses *Example: A user clicks an emailed link that installs ransomware*	The organization is at risk of infection from a specific type of ransomware that can somehow elude or defeat our defenses *Example: A user clicks a Facebook link that triggers a new type of ransomware network-wide*
Website Defacement	N/A	A secondary website is hacked *Example: simsburyforum.com is hacked*	A primary website is hacked *Example: simsbury-ct.gov is hacked*

Appendix D: Definitions

The following defined terms are used in this guide:

Availability	This is the 'property' of being operational, accessible, functional and usable upon demand by an authorized entity, e.g. a system or user.
Compromised	The disclosure of sensitive information to persons not authorized access or having a need-to-know.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources.
Firewalls	A combination of hardware and software which limits the exposure of a computer or group of computers to an attack from outside.
Integrity	The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.
ISP	Internet Service Provider (ISP) is an organization that provides Internet access.
Ransomware	A type of malicious software designed to block access to a computer system or its data until a sum of money is paid.
Routers	Devices that connect networks and direct the flow of data.
Unauthorized Access	Gaining access into any computer system or network without expressed permission of the owner.
Virus	A program written to alter the way a computer operates, without the permission or knowledge of the user. Infection requires the distribution of a host file.
Vulnerability Scan	The process where a computer or network is checked for security issues, missing patches or misconfigurations. The scan results are typically compiled into a report, identifying the vulnerability along with remediation steps to correct the issue.
Worm	A program written to alter the way a computer operates, without the permission or knowledge of the user. Infection does not require the distribution of a host file.