



Incident Response Plan & Computer Uses Policy

PURPOSE: To ensure that Information Technology (IT) properly identifies, contains, investigates, remedies, reports, and responds to computer security incidents.

POLICY: This policy is applicable to all departments and users of IT resources and assets.

1. INCIDENT RESPONSE TRAINING - The Town of Newport shall:
 - a. Provide incident response training to information system users consistent with assigned roles and responsibilities:
 - i. Within one week of assuming an incident response role or responsibility.
 - ii. When required by information system changes, and annually thereafter.
 - b. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.
 - c. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.
2. INCIDENT RESPONSE TESTING - The Town of Newport shall:
 - a. Test the incident response capability for the information system annually using appropriate tests to determine the incident response effectiveness and documents the results.
 - b. Coordinate incident response testing with entity contacts responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.
3. INCIDENT HANDLING - The Town of Newport shall:
 - a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
 - b. Coordinate incident handling activities with contingency planning activities.
 - c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.
4. INCIDENT MONITORING - The Town of Newport shall:
 - a. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.



5. INCIDENT REPORTING - The Town of Newport shall:
 - a. Require personnel to report suspected security incidents to the incident response capability immediately.
 - b. Report security incident information as follows: Suspicious emails, forward to the Town Manager, manager@newportnh.gov and the Newport Police Department at policechief@newportnh.gov. Unusual programs, screens, computer activity call the Town Manager's Office at (603) 863-1877; if outside of normal business hours call the Newport Police Department Dispatch at (603) 863-3232.
6. INCIDENT RESPONSE ASSISTANCE - The Town of Newport shall:
 - a. Provide an incident response support resource, integral to the incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.
7. INCIDENT RESPONSE PLAN - The Town of Newport shall:
 - a. Develop an incident response plan that:
 - i. Provides the Town of Newport with a roadmap for implementing its incident response capability.
 - ii. Describes the structure of the incident response capability.
 - iii. Provides a high-level approach for how the incident response capability fits into the overall Town of Newport.
 - iv. Meets the unique requirements of the Town of Newport, which relate to mission, size, structure, and functions.
 - v. Defines reportable incidents.
 - vi. Provides metrics for measuring the incident response capability within the Town of Newport.
 - vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.
 - viii. Is reviewed and approved by the Town Manager.
 - b. Distribute copies of the incident response plan to all system users.
 - c. Review the incident response plan annually.
 - d. Update the incident response plan to address technically unique incidents, system changes or problems encountered during plan implementation, execution, or testing.



- e. Communicate incident response plan changes to all system users.
- f. Protect the incident response plan from unauthorized disclosure and modification.

COMPLIANCE: Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions.

POLICY EXCEPTIONS: Requests for exceptions to this policy shall be reviewed by the Town Manager. Departments requesting exceptions shall provide such requests to the Town Manager. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The Town Manager shall review such requests and confer with the requesting department.

RESPONSIBLE DEPARTMENT: Finance Department

E. Use of Technology

1. All electronic and telephonic communication systems and all data, files, records, stored in Town equipment and systems are the property of the Town (hereinafter referred to in this Policy as “Town technology”. It is anticipated that Town technology devices will be utilized primarily to facilitate the delivery of municipal services and to assist in the day-to-day operation of the Town. All employees should be aware that the Town has the right, but not the obligation, to monitor, access, retrieve, restrict, publish or otherwise manage the use of Town technology at any time without regard to employee privacy issues. For this reason, employees cannot and should not expect privacy in their use of Town technology, and should instead expect that their e-mail messages, voice mail messages, computer and internet use, and other use of the Town’s technology is not confidential and may be monitored, reviewed and disclosed.
2. The use of Town technology devices for personal reasons shall be limited to infrequent occasions, breaks or non-work hours.
3. Improper use of Town technology devices may result in disciplinary action, up to and including discharge. Unacceptable uses of Town technology shall include, but are not necessarily limited to, the following:
 - The unauthorized transmission of highly confidential or sensitive customer or proprietary material outside of the office;
 - The unauthorized use for any business or commercial purposes other than the delivery of municipal services;
 - Misrepresentation or non-disclosure of an employee’s actual identity or



affiliation with the Town of Newport; unless authorized by law or as part of a criminal investigation.

- The unauthorized transmission of harassing, intimidating, abusive or offensive material;
 - The unauthorized disclosure, interception, disruption or alteration of electronic messages or data, including confidential, sensitive and non-public materials;
 - Soliciting, receiving or transmitting sexually explicit material of any type; unless authorized by law or as part of a criminal investigation.
 - Posting unauthorized newsgroup or bulletin board messages on behalf of or representing the Town;
 - Knowingly or purposely causing, excessive strain on any computing facilities or resources, or unwarranted or unsolicited interference with others' use of technology devices such as chain letters, viruses, spam, etc.;
 - Using technology devices for any purpose that violates federal or state laws, including but not limited to gambling, copyright violations or software licensing infringement;
 - The introduction or installation of any unauthorized software, hardware, discs, files, downloads, cookies, surveys, scans or other technology devices;
 - The incurring of any expenses or fees that are not specifically authorized by a Supervisor, or conduct which results in such expenses to the Town;
4. **Unauthorized Access:** Unauthorized access of Town technology is prohibited. Employees are not permitted to use a code, access a file, or retrieve any stored communication unless authorized to do so or unless they have received prior clearance from an authorized Town representative. Town computers and information technology is for business use by Town personnel. Non-employees may not use Town technology without permission from a Department Supervisor.
5. Use of another employee's account, user name, or password, or accessing another's files without their consent (by anyone other than authorized representatives of the Town) is strictly prohibited. Obtaining, or trying to obtain, other users' passwords, or using programs that compromise security in any way is prohibited.
6. Passwords are required for many of the applications of Town technology and users may be required to change passwords periodically for security purposes. All



passcodes and passwords are the property of the Town. No employee may use a passcode, password, or voice mail access code that has not been issued to that employee by the Town or that is unknown to the Town. Users of the Town's computers, network, and other technology must take reasonable precautions to prevent unauthorized access to the Town's technology resources. Passwords should not be divulged to unauthorized persons, and should not be written down or sent over the Internet, Intranet, e-mail, dial-up modem, or any other communication line.

7. **Snooping**: Probing or "snooping" into Town technology is prohibited. No employee may access the Town's files or any other files on the network or the system that the employee did not create unless the employee has prior authorization from his/her Supervisor or another authorized Town official. Observations of probing or "snooping" should be reported to the Town Manager.
8. **Sabotage**: Destruction, theft, alteration, or any other form of sabotage of Town technology and/or Town resources, including, but not limited to, computers, programs, networks, web-sites, files, and data is prohibited and will be investigated and prosecuted to the fullest extent of the law.
9. **Hacking**: Hacking, the breaking into and corrupting of information technology, is prohibited. Hacking into third party computer systems using Town technology is prohibited, and may be reported to the local authorities. Vulnerability in Town technology should be reported to the Town Manager.
10. **Viruses**: Use of virus, worm, or Trojan horse programs is prohibited. If a virus, worm or Trojan horse is identified, it should be immediately reported to the Department Head.
11. **Confidential Information**: Information sent to or from a Town computer may not in all situations be considered confidential information. It should be known that information sent to or from a Town computer may be considered a public document under provisions of NH RSA 91-a and the Federal Freedom of Information Act and care shall be given to protect confidential information. When sending e-mail messages concerning confidential and/or proprietary information, employees are expected to exercise significant caution because of the ability of others to "crack" the system. Questions regarding what level of security is needed for particular information should be directed to the Department Head or Town Manager.
12. **Safeguarding the Physical Security of Communications System**: Reasonable precautions should be taken in regards to the physical security of Town technology resources. Disks, drives, and other devices containing sensitive information should be contained in a locked drawer, wherever possible. Computers should be turned off when not in use for an extended period or when an employee is out of his/her office for extended periods of time.



13. All software installed on workstations, whether for business or personal use, must be approved by the employee's Supervisor. In no way should personal computer hardware (thumb drives, MP3 players, etc.) be installed on Town technology unless authorized by the employee's Supervisor. Purchases of computer software and equipment by anyone other than an authorized Town official are prohibited. Employees should not install Town software on home computers without the prior approval of Town Management.
14. Employees may not intentionally download anything from the Internet without prior authorization. This includes, but is not limited to, screensavers, music, E-mail stationary, and other images.
15. Copyright Infringement/Unauthorized Copying: The Town does not condone the illegal duplication of software or any violations of copyright laws.

F. **Social Media Guidelines**

1. The following guidelines are hereby enacted as a supplement to the Town's Use of Technology Policy as set forth in Section XVII.D of the Personnel Plan above).

These guidelines are to be construed as the Town's exercise of its management rights in the determination of the methods and means by which information, documentation, photographs, video, audio, data, electronic files, passwords, communications, and messages related to official government functions are to be publicly conveyed (or withheld from distribution) by Town employees through social media websites.

Any violation of these guidelines shall be subject to disciplinary action as otherwise set forth herein; to be consistent with the provisions of the Town's Personnel Plan and/or collective bargaining agreements as may be applicable hereto.

2. Social networking shall be defined as communicating and sharing information between two or more individuals in an online or internet community, such as the use of Facebook, Twitter, LinkedIn, YouTube, AOL, and similar websites. (These guidelines do not apply to private email accounts or the exchange of private text messages as may otherwise be allowed at appropriate times during the workday.)
3. Use of privately-owned computers or hand-held devices using the Town's internet connection services during the work day shall be allowed during authorized break periods only.
4. Unless authorized to do so by the Town Manager, employees are prohibited from using any social media websites to publicly display Town-owned badges, uniforms, logos, insignia, tools, equipment, vehicles or other images of Town-



owned property.

5. Unless authorized to do so by the Town Manager, employees shall not identify themselves or refer to other Town employees by job title, rank, classification or position when engaged in social networking, except as otherwise permitted by law, or when specifically authorized in writing by the employee's immediate supervisor for the exercise of official duties.
6. Employees shall not post, transmit or distribute any images obtained from a work place or while on-duty, to include scenes of accidents, crimes, fires, training sites or any other municipal activity except upon written authorization from the Town Manager. (This guideline does not apply to images made during a public meeting as otherwise allowed under RSA 91-A: 2. or as part of a formal press release made available to the media.) The unauthorized release or distribution of any photograph or video recording of an incident victim may be cause for immediate discharge as a Town employee. There may be cases whereby images or videos are taken to promote a municipal activity or an event, in such cases proper authorization shall be obtained to post to social media sites.
7. Employees who participate in social networking while off-duty shall maintain an appropriate level of professionalism and decorum when making reference to municipal operations or other Town employees, agents or officials.
8. The Town recognizes all employees have constitutionally protected rights pertaining to freedom of speech, freedom of expression, freedom of association, and protections afforded under the Whistle Blower's Protection Act. In addition, employees have a right to discuss their wages, hours and working conditions with co-workers and others. However, any social media displays of willful or deliberate malicious acts that result in the disruption of workplace relationships will be treated as though the behavior took place while in the employment of the Town. The following social media situations by employees are likely to result in the imposition of disciplinary action, up to and including discharge:
 - Behavior that is directed towards a Town official using language that is defamatory, slanderous or unlawful;
 - Conduct that interferes with the maintenance of essential work-place discipline;
 - Actions of an obscene or derogatory nature that damage or impair the reputation and/or efficiency of municipal operations;
 - Cyber-bullying directed towards any Town employee.
9. The Town reserves the right to investigate and obtain information about employees and candidates for employment by viewing social media website(s)



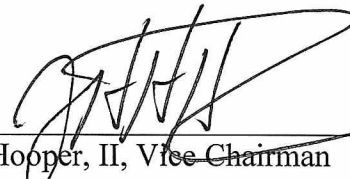
that are in the public domain. However, no Town Official shall engage in any activity regarding electronic media that is otherwise prohibited by RSA 275:74.

10. The use of private or personal social media shall not be considered part of the scope of an employee's duties except when authorized in writing by an employee's immediate supervisor. Accordingly, in most cases the Town shall not indemnify employees from personal financial loss and/or expense, including reasonable attorney fees, for any claims, demands, suits, or judgments resulting in damages arising from any matters that are published, posted, transmitted, broadcasted, displayed or disseminated on a private or personal social media website.
11. All social media communications by Town officials about governmental proceedings or the publication of governmental records shall be subject to the New Hampshire Right-To-Know Law and public access pursuant to the provisions of RSA 91-A, including, but not limited to (a) the obligation to preserve such records for specific time periods (usually measured in number of years); and (b) the remedies (and possibly penalties) as set forth in RSA 91-A: 8.

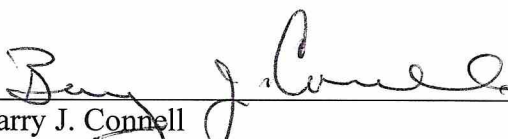
Adopted by the Town of Newport Board of Selectmen on: October 4, 2021



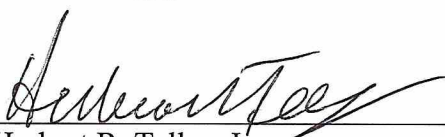
Jeffrey F. Kessler, Chairman



John H. Hooper, II, Vice Chairman



Barry J. Connell



Herbert R. Tellor, Jr.



Keith M. Sayer