**Town of Deep River**

**POLICY / PROCEDURE MANUAL**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Corporate Policies and Procedures** | | | | |
| **DEPARTMENT:** Administration | | | | **POLICY #:**  IT-05 |
| **POLICY:** Mobile Hardware Security | | | | |
| **DATE OF ORIGIN:**  Dec. 15, 2021 | **REVIEW DATE:** | **REVISION DATE:** | **APPLICABLE TO:**  All Employees | **PAGE #:** 1 to 2 |

**POLICY STATEMENT**

The Town of Deep River sets the following guidelines for its employees to protect the security and integrity of mobile computing devices.

**DEFINITIONS**

**Mobile Computing Devices**

Any easily portable device that is capable of receiving and/or transmitting data to and from information resources. These include, but are not limited to, laptop computers, tablets, and cell phones.

**PROCEDURE**

1. Portable computing devices located at Town sites must be stored in a secure environment after business hours. This may be a locked office, or locked desk drawer if not an office environment.
2. Mobile users are responsible to ensure the safety of mobile devices assigned to them. This encompasses ensuring the integrity and security of the physical environment, as well as Town data contained on said devices. All reasonable preventative precautions should be taken when travelling with Town owned hardware.
3. The System Administrator configures software security measures (i.e., local username and password) on all Town computers and devices. Do not alter or remove security measures as put in place by the Administrator.
4. The System Administrator maintains a comprehensive, detailed inventory of all corporate computer hardware and software. The accuracy of this inventory is critical in the event of a theft or loss issue. No user shall add, remove, or change the location or contents of any Town hardware without consultation with the Administrator. Only Town licensed software will be installed on Town hardware.
5. Should the employee’s laptop or portable device go missing, become lost or stolen, the employee should inform the Administrator as soon as possible.
6. Should a theft occur, and the employee responsible for the piece of hardware has neglected the above guidelines, the employee may be held personally liable for the replacement cost of the device.