TOWN OF BIG FLATS PASSWORD POLICY

1. PURPOSE

Town of Big Flats representatives are required to define and utilize strong passwords in order to protect their publicly accessible content.

2. DEFINITIONS

Representative: Any elected official of the Town of Big Flats; any appointee of the Town of Big Flats; and/or any employee of the Town of Big Flats.

Town System: Any computer system owned or leased by the Town of Big Flats; computing service operated for the Town of Big Flats; and/or electronic communication service operated for the Town of Big Flats.

3. POLICY

Representatives must adhere to the following rules when securing town systems and email accounts:

* Passwords must be at least eight characters in length.

* Passwords must include both uppercase and lowercase letters.

* Passwords must include at least one digit.

* The Town administration shall schedule overall password changes intermittently. The period between such changes shall not exceed 18 months

* Passwords must not be written down and placed in easily accessible locations.

* Machine and email passwords must not be the same.

* In general, reusing passwords diminishes the security of the systems they protect. To minimizes this risk, passwords may only be reused every third password, at minimum. As such a completely new password is required for the first two expires; thereafter, the first password can be reused. "Completely new" is defined as having at least fifty percent (50%) of the characters different from the previous password.

* Passwords for Administrative control that must be shared (main server, routers, general admin log-in) and external authentications, e.g. the BF website shall be kept by the Town Clerk and IT administrator and kept by them in a secure place known to each other. Passwords should never be posted in easily accessible areas such as on monitors or keyboards. Passwords are to be treated as confidential information and shall not be shared with non-authorized individuals. A record must be kept of the name of any individual the password(s) is/are shared

with and shall have the date of sharing as well as notations regarding new passwords and whether or not they were also shared.

* If an employee either knows or suspects that his/her password has been compromised, he/she must report it to his/her IT department and department supervisor, and must immediately change the password.

In addition

· The email host must be configured to enforce email password redefinition on a six month basis

· The email host must be configured to enforce password compliance levels.