



## **Information Security Policy**

Date of Origin: 08/14/2018

Modification Date(s): 11/10/20, 8/18/23

Date of Last Review: 11/12/24

### **I. Purpose**

The Information Security Policy establishes UCP's approach to ensure that the integrity of UCP information including client and organizational data remains intact and that efforts are taken to detect and preempt any misuse of data, networks, IT systems and applications.

### **II. Scope**

This policy applies to all information, information systems, networks, applications, locations and the users of each.

### **III. Definition**

The following UCP information is classified as confidential:

- All client information including name, address, contact information, social security number, date of birth, insurance, diagnosis, documentation of care or other protected health information (as defined by HIPAA)
- Employee address, date of birth, social security, bank account number, driver's license number, pay, or any other protected health information (as defined by HIPAA)
- Organizational information related to processes, operations, financial accounts and transactions, profits, losses, expenditures, or other information for which the disclosure of which is likely to have a negative effect or cause substantial harm to the organization

### **IV. Policy**

All employees, contractors, and volunteers have a responsibility for proper handling and protection of confidential information. These responsibilities include but are not limited to:

- Protecting passwords and other access credentials from unauthorized use for any UCP device ensuring passwords contain 12 or more characters, upper and lower case letters, at least one number and one symbol
- Accessing systems and information on a need-to-know basis only and for authorized use only
- Locking computer screens when not in use or stepping away from computer
- Appropriately protecting electronic or physical records containing client, employee or other UCP confidential information when transported or transmitted,

including the use of secure/encryption when communicating confidential information via email

- Properly disposing of electronic or physical confidential records so that the information cannot be retrieved when no longer needed or required to be kept
- Reporting any actual or suspected loss, theft or improper use of or access to UCP confidential information
- Ensuring bit locker encryption is in place for all computers that leave the building
- Ensuring cell phones used for work purposes are passcode protected
- All Data storage devices that leave the building need to be encrypted and password protected, such as flash drives, external hard drives, memory cards, and other Data storage devices.
- Administrator account logins will have multi-factor authentication.

### **Cyber Security**

The following actions must be taken by staff as appropriate to ensure the integrity of UCP IT systems remain unharmed:

- All suspicious emails must be reported to UCP's Information Technology department and should not be opened until deemed safe by IT staff.
- Any requests for UCP confidential information (including usernames and passwords) will not be responded to without internal verification of the requesting source and appropriate next steps. At no time will login information be shared with anyone other than designated IT staff and must be immediately changed after access is granted and no longer needed by designated IT staff.
- When entering confidential information into websites, ensure that the address listed begins with https://. Any web address that does not include the "s" is not a secure site.
- Never visit sites while on UCP devices or UCP network that are not work-related and notify IT of any suspicious sites that are accessed accidentally.


### **User Access**

Access to information, information systems, networks, and applications will be limited to those individuals who have a bonafide business need to access the information. Access to information housed electronically in networks or UCP applications will be controlled by UCP's Information Technology staff with oversight by the CEO and Director of Operations.

Any application or website deemed a potential threat to UCP IT infrastructure will be restricted for use by employees while on the UCP network or at all times if using UCP provided technology.

### **V. Policy Violations**

Any violations of the IT Security Policy may result in disciplinary action, up to and including termination depending on the level of infraction and risk associated with the infraction.

  
\_\_\_\_\_  
Scott Tash, CEO

  
\_\_\_\_\_  
Date