CRFPD CYBER LIABILTY POLICY

The primary goal in mitigating risk in a digital environment is to safeguard the sensitive data. The data considered sensitive to the CRFPD would be any RRV information regarding grades or reimbursement contracts. These typically are stored in paper form in a locked cabinet. Therefore, no electronic or cyber version of this sensitive data should exist. It is the policy of the CRFPD that should any data ever be classified as "Cyber Sensitive" we will:

1. Safeguard the data:

a. Identify and empower a key employee(s) to own the responsibility of safeguarding sensitive data.

b. Identify the data that is being received, transmitted and stored. What type of data - PI, PHI, and/or PCI?

c. Identify how and where the data is being received or generated (email, cloud services, user devices, etc.). Data should only be received or generated if there is a legitimate business reason to do so.

d. Identify how and where the data is being stored (network servers, user devices, removable media, cloud services, physical filing systems, etc.). Data should only be stored if there is a legitimate business reason to do so.

e. Identify how the data is being protected. If it is sensitive data, consider encryption in both transit and at rest.

f. Identify how and when the data is being disposed. Data should only be kept as long as there is a legitimate business reason to retain it, and it should thereafter be securely shredded or degaussed.

2. Safeguard the information Systems

a. Identify and empower a key employee(s) to own the responsibility of safeguarding the information system – it may be the same person(s) responsible for safeguarding the data, but there must be someone empowered and resourced to protect the system.

b. Inventory authorized hardware to help detect unauthorized devices. You have to know your network – know what should be on it - in order to protect it.

c. Inventory authorized software to help detect unauthorized and malicious software. Similar to hardware, you have to know what should be on your network in order to detect and prevent unauthorized software.

d. Develop and implement secure configurations for all devices to reduce the number of vulnerabilities an attacker could exploit.

e. Continuously monitor for and assess vulnerabilities and immediately remediate. The digital environment is in a constant state of flux, and the threats continue to change in scope and severity. It is therefore critical that you continuously seek to identify vulnerabilities, and immediately remediate them.

f. Control use of administrative privileges to ensure that only those employees with legitimate occupational need are allowed administrative access to network resources and devices. Control access based on the need to know to prevent unauthorized access to the system and data.

g. Actively monitor and control all active accounts to minimize authorized access. • Review all accounts and disable inactive accounts;

• Ensure all employee accounts are terminated immediately upon an employee’s departure;

• Ensure all contractor accounts are terminated upon completion of the project;

• Ensure all service accounts are secured if used or terminated if inactive. h. Actively protect all accounts and user devices.

• Implement password complexity rules requiring passwords to meet length and strength requirements, including a mix of uppercase and lowercase letters, numbers, and symbols;

• Require passwords to be changed routinely and kept private;

• Encrypt devices to protect sensitive data;

• Require screen locks after short intervals of inactivity.

i. Implement email and web browser protections to mitigate the risk that unauthorized users could compromise your system.

a. • Use only fully-supported web browsers and email clients in your organization;

b. • Use spam filters and firewalls to prevent unwanted, harmful email, and other forms of potentially vulnerable communications.

j. Use anti-malware software to prevent malicious programs like ransomware from being entering or being installed in your environment.

k. Deploy boundary defenses, including firewalls, to control the flow of traffic and search for evidence of unauthorized access or malicious programs.

c. • Create blacklists of known malicious IP addresses and deny them access;

d. • Create whitelists of known, trusted sites that employees should or need to have access to from organization devices;

e. • Use a VPN or other secured means for users to remotely access your organization’s network;

f. • Require multi-factor authentication for all remote access to your organization’s network.

l. Monitor both inbound and outbound traffic. It is important to not just monitor what is entering your network, but it is increasingly important to monitor what is leaving your network. Unauthorized users often enter through encrypted tunnels, and are not detected until they attempt to leave with sensitive data.

m. Strengthen the security of your wireless networks and limit wireless access to your network to authorized devices with a bona fide business need.

Adopted at the regular CRFPD Board of Directors’ Meeting on October 24, 2017
Attested to by Bob Conder, Chairman