**MEMORANDUM**

To: Chief Information Officer

From: Team

Subject: Due Care

Date:

Team has prepared the following statement of Due Care for the organization to be reviewed with the General Counsel and Attorneys:

**Introduction**

Due Care is the conduct that a reasonable person will exercise in a particular situation in looking out for the protection of things or the safety of others. It is a simple concept, and it is an important one.

At our organization, we have good reason to be conscientious about providing due care for the information that fuels intellectual inspiration, collaboration, and innovation. In our security team, we continually develop processes and methods to appropriately and responsibly handle our collective data and the duties that accompany it.

**Proper Standards, Policies, and Procedures**

The organization abides by the policies and standards in the NIST CSF framework and ISO 27001 as the foundation of our cybersecurity program. We’ve additionally developed mature security processes to protect each type of user data that is protected by law or regulation. These processes include a thorough and robust risk assessment plan that is regularly reviewed and audited, security assessments as required by third-party assessments, and engaging in cybersecurity insurance providers.

**Cybersecurity Awareness Training**The organization provides cybersecurity awareness training for all organization staff, contractors, vendors, business partners, advisors, and board members prior to being granted access to the organization’s data and information technology resources. The training address es roles, responsibilities, management commitment, proper disposal of data storage media, coordination among organizational entities and compliance. Special focus is given to sensitive system and data concerns.

**Data Loss Prevention**

The organization has a special focus on their Data Loss Prevention policy to protect the integrity and confidentiality of sensitive user data. Sensitive information may include financial records, customer data, credit card data, or other protected information. This policy is routinely updated to emerging rules, regulations, and standards.

**Protecting Data From Breaches**

Our Data Loss Prevention policy in accordance with the standards in the NIST CSF framework and ISO 27001 will help to prevent data being accessed by those outside our organization. Our security team continually monitors access to our machines and the flow of information between devices to determine if there is unauthorized access to critical data storage. If there is unauthorized access detected our security team will be notified and will block that connection providing access to the data.

**Continuous Controls Monitoring and Refinement**

Controls, policies, and procedures are regularly reviewed and refined to protect user and organizational data. If needed, controls are modified and improved according to the organization’s control improvement plan.

**References**

The following articles provided insight to creating this Due Care statement:

* Due Care and Due Diligence: <https://www.centraleyes.com/the-difference-between-due-diligence-and-due-care-in-cybersecurity/>
* Due Care at another organization: <https://ciso.uw.edu/policy/due-care/>
* Security Awareness at another organization: <https://vsu.edu/files/docs/policies/6000/6530-security-awareness-training.pdf>
* Due Care at another organization: <https://www.uapb.edu/sites/www/Uploads/files/PDFs/DATA%20LOSS%20PREVENTION.pdf>

Please let us know if there are any other actions we can perform to help prepare our attorneys for their Due Care statement at this time.

Thank you,

Team