Cybersecurity Governance Charter

# Institution Name

## **Governance Committee Representatives**

#### Below are roles or areas that should be represented in your governance committee. This list can be customized to fit the needs/structure of your institution. Depending on the size of your teams, more or less representation may be needed.

|  |  |
| --- | --- |
| **Role/Representative Area** | **Name** |
| Chief Information Officer |  |
| Chief Information Security Officer |  |
| Chief Privacy Officer/Data Officer |  |
| Human Resources |  |
| Risk Management |  |
| General Counsel |  |
| Business and Finance |  |
| Cybersecurity Director |  |
| Faculty Representative |  |
| IT Director(s) |  |
| Dean of Students |  |
| Campus Law Enforcement |  |
| Enterprise Infrastructure |  |
| Network Infrastructure |  |

## Purpose/Authority

In this section, define the purpose of this group and its areas of authority. Carefully define items both in and out of scope for the group.

## Guiding Principles

What are the core principles that will guide the group? How do they tie in with the institution’s mission, vision, and/or values? Examples include accountability, transparency, continuous improvement, cross-functional collaboration, etc.

## Areas of Responsibility

What are the responsibilities of this group? Examples include data governance, policy development/review, disaster recovery, business continuity, compliance risks, audits, reporting, advisory capacity, legislative/regulatory review, incident management and response planning, etc.

## Goals and Objectives

Depending on the existing structures of your institution, these could be short, mid, or long-term goals. Include how each goal or objective will be measured for success.

## Definitions

Are there any terms in the charter that should be defined for greater transparency? Include definitions and their specific context for your institution.