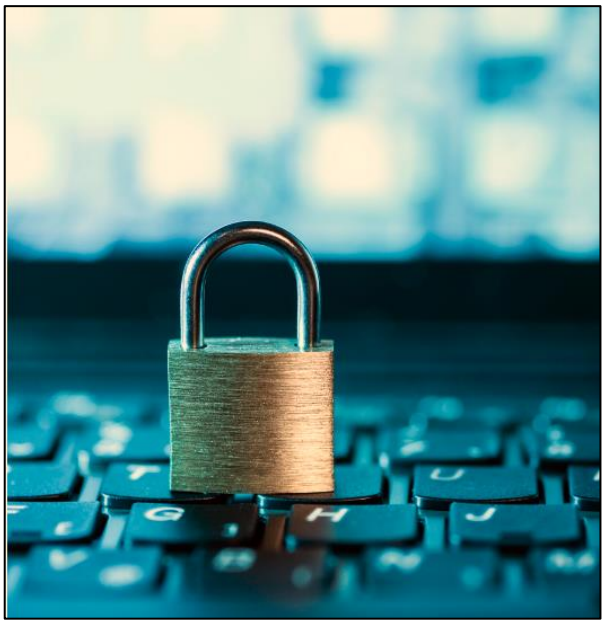
Vision 2 | Planned and Secure Technology Environment



A complex technology environment, and SMC's reliance on said environment, creates significant institutional risk. Breaches of the College's systems or a loss of service could have impactful ramifications on College operations and reputation.

During the assessment phase, BerryDunn noted multiple opportunities to reduce risk to SMC, including: establishing business continuity and DR plans, policies, and procedures that enable the institution to operate during outages and failures of critical systems; completing critical security projects and developing an information security program; and increasing awareness of IT governance to help ensure a tightly integrated and understood process across campus.

This section includes the following initiatives:

1. **Clarify, document, and refine governance and planning processes** – Define the IT governance structure and planning processes to improve clarity about how technology projects and priorities are established at SMC. This will serve to improve buy-in, engagement, coordination, and oversight of technology planning and decision-making.
2. **Develop an information systems security program** – A security program improves information security policies, processes, and tools, resulting in reduced risk to the College.
3. **Establish business continuity and DR plans** – Support institutional leadership in developing a comprehensive plan to maintain critical IT systems in the event of unplanned incidents. This will serve to reduce risk to the College.

Vision 2 | Planned and Secure Technology Environment	**2.2 | Develop an Information Systems Security Program**

Develop a framework to reduce institutional risk by establishing documented IT policies and procedures, regularly scheduled assessments/scans, and security awareness training.

Action Items to Implement Initiative

SMC will establish an Information Security Program based on National Institute of Standards and Technology (NIST) 171 standards that includes the following:

- An established information security office
- Security breach response plan
- Regular security assessments and third-party audits
- Center for Internet Security (CIS) critical controls assessment
- Phishing assessment
- Service policy and procedure catalog
- Vulnerability management
- Daily Splunk logging, Spirion data inventory and monitoring, and spam filtering
- Self-service password management/multi-factor authentication
- Mandatory security awareness training—included during new employee onboarding
- Secure Socket Layer (SSL) certificates
- Plan for mobile device management
- Approval process for data requests—data access management
- Encryption of protected data in transmission or at rest

Measures of Success

- 100% of employees have taken security awareness training.
- Security assessments and remediation efforts completed.
- Compliance with NIST standards and industry compliance requirements (Payment Card Industry (PCI), Gramm-Leach-Bliley Act (GLBA), General Data Protection Regulation (GDPR), etc.)

Primary Linkage to the SMC Strategic Initiatives	Level of Effort and Budgetary Considerations	Organizational Impact
Improve facilities and technology infrastructure, integration, and staffing	🧍 - Significant effort to establish, maintain, and execute information systems security program. May require additional funding.	●●● - District-wide. Everyone is responsible for information security.

Key Initiative Stakeholders	
Initiative Owner	Information security officer
Consultative Role	Senior staff, chief director of IT, IT staff, functional stakeholders

Vision 2 | Planned and Secure Technology Environment	**2.3 | Establish Business Continuity and DR Plans**
Develop a comprehensive plan to maintain critical IT systems in the event of unplanned incidents. IT can support the creation of an institutional business continuity plan, but the plan needs to be driven by the College leadership team.	

Action Items to Implement Initiative

- Conduct a business impact analysis to establish recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical systems.
- Conduct an analysis of existing datacenters and develop options for primary and backup sites moving forward. Assess costs of backing up directly to the cloud and determine frequency of backups.
- Procure funding and contract with an additional internet service provider for redundancy.
- Assess bandwidth requirement to support continuity of WebISIS.
- Develop an IT incident management/response team and communication plan that includes stakeholders from outside of IT.
- Document incident response scenarios and remediation plans. Maintain printed copies.
- Investigate and develop mutual aid agreements with external partners and institutions.
- Implement a test environment and test established plans regularly, including mock disaster drills. Stakeholders from outside of the department will need to participate. For example, facilities may need to assist with generator tests.
- Update plans on an annual basis.

Measures of Success

- Documented policies and procedures approved and in place.
- Adherence with established RPOs and RTOs during routine DR tests.

Primary Linkage to the SMC Strategic Initiatives	Level of Effort and Budgetary Considerations	Organizational Impact
Assure an effective and dynamic College by ensuring long-term fiscal stability.	**<** 🧍 - Effort – Significant effort by multiple stakeholders at the College to establish plans. Additional funding likely required.	●● - District-wide impact in the event of a disaster or unplanned outage.

Key Initiative Stakeholders	
Initiative Owner	TBD. This is not solely an IT initiative. SMC leadership needs to define an initiative owner.
Consultative Role	Senior staff, Chief director of IT, manager of information systems (MIS) manager, information security officer (ISO), IT staff, department heads