Committee 36-6 Information Security Approved Recommendations

1. Recommends that GSU adopt the Gartner Information Security Governance (ISG) model. This includes establishing governance bodies with clear goals, scopes of control and guidance, and ensuring the appropriate level of membership in these bodies is maintained over time.

2. Recommends that GSU adopt the ACUPA model for policy development, which aligns with the NIST standards, BOR IT Handbook, and GTA policy models in use currently. It is also recommended part of this initiative should include a comprehensive review, consolidation and reconciliation of all current security policies for both institutions.

3. Recommends that USG contract with a commercial Managed Security Services Provider (MSSP) for operations security monitoring and incident management.

4. Recommends that GSU utilize the Gartner ITScore methodology to conduct assessments of organizational security domains for security program maturity analysis and planning.

5. Recommends the development of a strategic plan to guide the direction of the information security practice.

6. Recommends that a risk assessment be performed on all colleges and business units.

7. Recommends that GSU InfoSec develop a training and education plan for department security practitioners, including training for the planned extended security team and ISO’s within the colleges, business units, extended IT and IS&T.

8. Recommends that a comprehensive review of all current Information Security projects and initiatives for both institutions be conducted.

9. Recommends that the Change Management function within IS&T should be realigned within the organization and moved from the InfoSec office where it currently resides, to the PMO function.

10. Recommends a review of all security-related tools and solutions being utilized throughout the enterprise at both institutions. This review should be conducted within the areas of IT, including enterprise systems, network and infrastructure, application development, client services (helpdesk support and desktop engineering), and the project office, to get overall consensus. Second phase review will be extended to the distributed IT units.

11. Recommends that GSU invest in a commercial Web Application Firewall tool for protection of the web and application development, and production environments.
12. Recommends that GSU invest in a commercial Database Activity Monitor, a proactive, automated protection, audit, and compliance tool.

13. Recommends that GSU invest in a Security Information Events Monitor (SIEM) tool, used in security operations for malicious threat detection, aggregation and correlation, alerting, and logging.

14. Recommends that GSU invest in a content-aware Data Loss Prevention (DLP) tool.

15. Recommends that IS&T select and standardize on a unified asset lifecycle management platform. This solution must include automated asset discovery; have the ability to identify all manner of network-connected devices; and be utilized as an enterprise configuration and vulnerability management tool.

16. Recommends that GSU and GPC standardize on an endpoint security solution that meets the compliance requirements of the BOR IT Handbook, and which also covers security best practices for computing endpoints.

17. Recommends investment in a network firewall and switch audit tool to automate and simplify security operations including troubleshooting, auditing and risk analysis, allowing for optimization of the configuration of firewalls, routers, load balancers and web proxies to ensure security and compliance.

18. Recommends that GSU networking and infrastructure, design and implement a new network for the newly consolidated institution, allowing for a move away from the legacy designs of old, to a modern network, designed and built with security at its core, to defend against modern malware and the way networks are attacked today.

19. Recommends that GSU unify on a common security-training platform for delivery to meet awareness, training, and education needs and requirements.

20. Recommends that GSU standardize on a coherent device-naming scheme.