Encryption Policy – March 25, 2007

Purpose: Explore expanded use of encryption alternatives and strategies, particularly related to email exchange and data storage.

IT Council recommends that VSC IT staff deploy standard encryption technologies to IT servers/services involved in the transmittal or storage of sensitive data. Careful consideration and extensive testing must be done before full-scale deployment of encryption is installed on any VSC systems, particularly those involved in serving a large population of users (i.e., Colleague, Maple, Blackboard, payroll, email, file/print services).

We also acknowledge that some servers/services that transmit or store sensitive data cannot be encrypted and still continue to perform their business function. Documentation of these instances and other protective measures will be necessary in these cases. There will also be cases where encryption is possible, but performance is significantly, negatively affected. In these cases, the risk of not encrypting will have to be weighed against the loss of productivity and customer service impact.

Finally, it will be the case that implementation of encryption for some applications will require new hardware or software to support the encryption technology.

Implementation steps should include:

- Identification of the standard encryption tools that will be used by the VSC.
- Use of SSL certificates with a minimum of 128-bit encryption installed on all systems offering access to the web and requiring a web login.
- Investigation of options for becoming an official Certificate Signing authority for SSL certificates.
- Use of an encrypted version of ftp and telnet whenever sensitive data is transmitted, either on or off the VSC network.
- Encrypting client/server operations with a vendor-supported version of software that permits application operation without degraded performance. Systems should be upgraded with necessary hardware/software to support encryption technology.
- Encryption of all drives (desktop, laptop, and other devices) except for servers and physically secured archive data. Laptop encryption will begin this process.
- An exception for public computers, differentiating between library and lab computers.

We do not recommend the encryption of email. It will introduce technical communications issues within and outside of the VSC and will not significantly improve the security of sensitive data. Implementation of other policies to restrict the use of email for the transmission of sensitive data, user training programs, email retention policies, and protection of sensitive data on servers is our recommendation to address this issue.