Defining an encryption standard for UCLA

Encryption is seen as a means to protect data and to help implement security for the purpose of regulatory compliance. However, there are a variety of encryption products, techniques and limitations, with little guidance in the law as to what is reasonable or sufficient. Further, whatever is chosen should have applicability to a wide variety of devices and media – from large database servers to laptops to PDAs to iPods.

People all over campus are now implementing one encryption tool or another without understanding the big picture. It is important for UCLA to have an “encryption standard” that all could reference if they are considering encryption as a security technique for stored data. Whether this standard would be defined in terms of software tools, encryption techniques or some other criteria remains to be determined; but whatever the standard is, it must satisfy not only technical reasonableness, but also reasonableness in legal, management and usability terms. There may also ultimately be savings to be gained from negotiated licensing agreements.

Proposed process

Convene a group(s) to:

- Understand the basic legal and regulatory requirements
- Understand the managements issues
- Survey the technology landscape for encryption
- Identify which situations encryption is most effectively employed

and to provide:

- A summary of findings
- A recommendation for an encryption standard or recommendations for next steps as appropriate.

Participants would be drawn from Campus Counsel, records management, information technology, internal audit and others as appropriate.