Data Transmission (including Encryption)

Data Transmission (including Encryption)

Why is this Important:
Similar to data use provisions, an institution of higher education may want to consider data protection provisions that stipulate how a contracting third party electronically transmits institution data. This type of provision can help protect the institution in event of a data breach (by providing an encryption safe harbor) or contractual breach.

Reference:
Appendix 1 ISO/IEC 27002:2005, Reference 6.2.3(b)(6)
Appendix 2 NIST Sp. Pub. 800-53, Rev. 2; Control SC-8 (Transmission Integrity); SC-9 (Transmission Confidentiality)

Overview:
Appropriate transmission integrity and confidentiality is required by some contracts, particularly where the third party is initiating the transfer.

Criticality: Category 2 and Category 3 (Category 1 for cases such as credit card data).

Sample RFP Language:

1. How does Institution data go between Institution and Proposer's proposed system? If connecting via a private circuit, describe what security features are incorporated into the private circuit. If connecting via a public network (e.g., the Internet), describe the way the Proposer will safeguard Institution data.
2. Does the product secure the data transmission between Institution and the Proposer? If yes, describe how the Proposer provides that security. If no, what alternative safeguards are used to protect Institution data in transit?
3. Does the product secure the communications between the managed systems or administrators to the centralized manager server? If yes, describe how the product provides that security.
4. Does the product encrypt Confidential data in transit and at rest? If yes, describe how the product provides that security. If no, what alternative methods are used to safeguard Confidential data in transit and at rest?
5. Does the Proposer protect Institution data backups against unauthorized access? If yes, describe the methods used by the Proposer to provide that protection.
6. Does the Proposer encrypt Institution data backups? If yes, describe the methods used by the Proposer to encrypt backup data. If no, what alternative safeguards does the Proposer use to protect Institution data backups against unauthorized access?

#Top

Sample Contract Clauses:

1. [Vendor] agrees that any transfer of data between the Institution and [Vendor] or within [Vendor]'s computing environment will take place using encrypted protocols such as SSL, step or scup.
2. [Vendor] certifies that all data backups of the Institution's data will be stored and maintained in an encrypted format using at least a 128 bit key.
3. [Vendor] will use only secure methods to access and electronically transfer Institution data files such as Secure or Securest from the Institution location and the [Vendor] location.
4. [Vendor] will use all reasonable practices and security procedures necessary to protect all electronic data that is transmitted between those parties under this Agreement by (but not limited to) electronic transmission or the physical delivery of electronically recorded data. Such protective measures shall include, but not be limited to, use of up-to-date anti-virus software to guard against viruses, worms, Trojan horses or other malware that may permit unauthorized access to data or may compromise the confidentiality, integrity or authorized accessibility of data or associated information systems of the other party. Neither Institution nor [Vendor] shall introduce into electronic data transmitted between them under this Agreement any virus, worm, Trojan horse or other malware that may permit unauthorized access to data or may compromise the confidentiality, integrity or authorized accessibility of data or associated information systems of the other party. Provided, however, in no event shall Institution be responsible for any damages or loss caused by electronic data transmitted to [Vendor].

#Top

common security items
