

Number:	Security Practice Bulletin #1 (SPB-1)
Title:	Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices.
Date:	June 1, 2007
Purpose:	<p>The purpose of this University of Texas System Information Security Practice Bulletin is to:</p> <ol style="list-style-type: none"> 1) establish encryption as a requirement in the event that Confidential University Data are to be stored on a Portable Computing Device or a Non-University Owned Computing Device, and 2) specify practices to ensure that there is a legitimate need before Confidential University Data are stored on a Portable Computing Device or a Non-University Owned Computing Device and that the Owner and User can ensure that encrypted data remain accessible in the event that an encryption key becomes lost or forgotten.
Definitions:	<p>Confidential Data: Data maintained by state agencies and universities a) of which unauthorized disclosure/use could cause serious damage to an organization or individual or b) that are exempt from disclosure under the provisions of the Public Records Act or other applicable state and federal laws. The controlling factor for Confidential Data is that of disclosure.</p> <p>Confidential University Data: Confidential Data maintained by an Entity of The University of Texas System.</p> <p>Entity or Entities: The University of Texas Institutions, System Administration, and UTIMCO.</p> <p>Non-University Owned Computing Device: Any device that is capable of receiving, transmitting, and/or storing electronic data and that is not owned or leased by or under the control of an Entity of The University of Texas System.</p> <p>Owner: The manager or agent responsible for the function that is supported by the resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared.</p> <p>Portable Computing Device: Any easily portable device that is capable of receiving, transmitting, and/or storing electronic data. This includes but is not limited to, notebook and tablet computers, handheld computers, personal digital assistants (PDAs), pagers, cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs, magnetic tapes, and similar storage devices.</p> <p>User: An individual, automated application or process that is authorized by the Owner to access the resource, in accordance with the Owner's procedures and rules. Has the responsibility to (1) use the resource only for the purpose specified by the Owner, (2) comply with controls established by the Owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized by the Owner of the information to read, enter, or update that information. The user is the single most effective control for providing adequate security.</p>

<p>Rationale:</p>	<p>Experience demonstrates that many incidents involving unauthorized exposure of confidential data, such as social security numbers and personal health information, are the result of stolen or lost Portable Computing Devices and Non-University Owned Computing Devices. The best way to prevent these exposures is to avoid storing confidential data on these devices. However, in situations that require Confidential University Data be stored on such devices, use of encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.</p> <p>While encryption mitigates risk of unauthorized data exposure, encryption can result in loss of access to the data by authorized Users, therefore procedures to mitigate this risk are also necessary.</p>
<p>Expectations:</p>	<ol style="list-style-type: none"> 1. As a general practice Confidential University Data are not to be copied to or stored on a Portable Computing Device or a Non-University Owned Computing Device. 2. Specific permission must be obtained from the data Owner before a User may store Confidential University Data on a Portable Computing Device or a Non-University Owned Computing Device. Such permission should be granted only upon demonstration of a business need and an assessment of the risk of unauthorized access to or loss of the data. 3. Any Confidential University Data stored on a Portable Computing Device or Non-University Owned Computing Device must be encrypted using products and/or methods approved by the Entity's Chief Information Security Officer (CISO or ISO). 4. Data Owners and Users of Portable Computing Devices and Non-University Owned Computing Devices containing Confidential University Data must acknowledge how they will ensure that data are encrypted and how encrypted data will be accessible by the Owner in the event that an encryption key becomes lost or forgotten. Various methods may be used to meet this requirement including: <ul style="list-style-type: none"> o Maintaining an accessible copy of the data on a server managed by the Entity, using procedures specified by the Entity. o Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key. o Escrowing the encryption key with a trusted party designated by the data Owner or the Entity's Chief Information Security Officer. o Use of other methods approved by the Entity's Chief Information Security Officer.
<p>Exceptions:</p>	<p>Under certain circumstances the CISO of the Entity may grant or issue an exception to the use of encryption on Portable Computing Devices and Non-University Owned Computing Devices containing Confidential University Data.</p> <p>Exceptions are of two types: 1) An exception may be granted to address the specific circumstances or business needs relating to an individual program or department. Requests for exceptions of this type should be in writing and should be initiated by the data Owner. 2) Broader exceptions may be issued to cover circumstances that span the Entity as a whole. Requests for exceptions of this type may come from any person, or such exceptions may be initiated by the CISO.</p> <ul style="list-style-type: none"> • All exceptions must be based on an assessment of business requirements weighed against the likelihood of an unauthorized exposure and the potential adverse consequences for individuals, other organizations, or the Entity were an exposure to occur. • As a condition for granting an exception, the CISO of the Entity may require compensating controls be implemented to offset the risk created by the lack of encryption. • Exceptions must be documented and must include the following elements: <ul style="list-style-type: none"> o A statement defining the nature and scope of the exception in terms of the data included and/or the class of devices included, o The rationale for granting the exception, o An expiration date for the exception, o A description of any compensating security measures that are to be required. o The signature of the CISO of the Entity, and in the case of an exception resulting from a data Owner request, the data Owner's signature.