



UCIT INFORMATION SECURITY STANDARDS

Two-Factor Authentication

Classification	Information Management	Table of Contents	
Standard	ISS-002	Rational	1
Approval Authority	Chief Information Officer	Scope	2
Implementation Authority	Information Security Office	Definition	3
Effective Date	July 7, 2009	Standard	4
Latest Revision	July 7, 2009	Exceptions	5
		Parent Policy	6
		Related Policies	7
		& Standards	
		History	8

Rationale	1	<p>The University has a duty to protect confidential information in its care. An important aspect of this is ensuring that users accessing this information are in fact who they claim to be.</p> <p>The traditional “one factor” authentication methods (where the credentials consist of only a username and password method) suffer from several weaknesses.</p> <ul style="list-style-type: none"> • Credentials can be divulged to others, deliberately or accidentally. • A credential can be “stolen” without the knowledge of the owner, e.g. via phishing, keystroke-logging, or simply watching over a user’s shoulder. • Multiple people can be in possession of the credentials at the same time. • Credentials can be “guessed” via brute-force or other means. <p>Two-factor authentication overcomes these weaknesses by requiring the user to provide a second factor that cannot be shared or duplicated.</p>
Scope	2	<p>This standard applies to all systems containing University of Calgary confidential and/or highly confidential data.</p>
Definitions	3	<p><i>Confidential Data:</i> Information classified as “Confidential” in accordance with the University Information Security Classification Standard.</p> <p><i>Highly Confidential Data:</i> Information classified “Highly Confidential” in accordance with the University Information Security Classification Standard.</p> <p><i>Two-Factor Authentication:</i> An identification verification scheme that requires the user to provide both a password and a token to prove that they are who they claim to be.</p> <p><i>Token:</i> The second factor in a two factor authentication system. Can be a physical device, a software-based code generator, or a biometric characteristic that corroborates identity assertions.</p>
Standard	4	<p>4.1. Required Use of Two-Factor Authentication</p> <p style="padding-left: 40px;">4.1.1. Users must authenticate themselves using an approved two-factor authentication scheme in order to access confidential or highly</p>

confidential data.

4.2. Management of Two-Factor Authentication Systems

4.2.1. In the case of physical and software-based tokens, there must be a controlled process for both the assignment and distribution of tokens to specific users.

4.2.2. In the case of biometric tokens, there must be a controlled process for associating biometric data to specific users.

4.2.3. Assignment must be attested to on an at least an annual basis by the token holder's supervisor.

4.2.4. Physical and software-based tokens must be assigned to a particular user before distribution.

4.2.5. Unassigned physical tokens must be kept physically secure.

4.2.6. An inventory of all physical tokens distributed and on-hand must be maintained for auditing purposes.

4.2.7. Tokens returned or reported lost, stolen, or damaged must be disabled immediately.

4.2.8. Tokens must be recovered from individuals who no longer have a legitimate need for them.

4.3. User Responsibilities

4.3.1. Users must not share their tokens with others.

4.3.2. Users must exercise due care to protect their tokens from loss, theft, and damage. Lost, stolen, or damaged tokens must be reported to the UCIT Support Center.

4.3.3. Users must return tokens no longer needed to the Support Centre.

Exceptions	5	4.1. Users may access confidential information about themselves (wherever they are entitled to do so) without the use of two-factor authentication.		
		4.2. The CIO can approve other exceptions to the above standard. Exemption requests must include detailed descriptions of:		
		a. Why the exception is necessary.		
		b. The compensating logical and physical security controls which will be used to ensure the protection of confidential data.		
Parent Policy	6			
Related Policies & Standards	7	<i>Information Asset Protection Policy</i>		
		<i>Information Asset Management Policy</i>		
		<i>Information Security Classification Standard</i>		
History	8	July 9, 2009	Jeremy Mortis	Created