

	Effective Date:	09-12-2011	
	Policy #:	G-19	
	Supersedes:		
Subject: Information Privacy and Security Encryption		Page:	1 of 2

PURPOSE

As custodians of data for Michigan’s citizens, Department of Licensing and Regulatory Affairs (LARA) employees are obligated to protect their private information. As more information becomes digitized, the risks of unauthorized disclosure or access increase. When information is e-mailed or sent to accounts or networks outside of state government, the security risk becomes much higher.

Requirements

The Department of Technology, Management and Budget (DTMB) is responsible for managing the state’s information technology (IT) resources. DTMB has issued [DTMB IT Information Security Policy 1340.00.07](#), which sets forth a basic electronic encryption policy for state IT resources handling confidential or restricted data.

Confidential or restricted data is that data connecting a person’s name with the person’s (a) social security, taxpayer identification, or driver’s license number, (b) medical information, (c) financial information, or (d) other information designated as confidential or restricted by standards, rules, regulations or laws.

Bureau directors shall designate a Data Steward who shall oversee the classification of data as confidential or restricted in different LARA work areas. LARA employees needing to electronically transfer confidential or restricted data to outside parties should consult with the Information Privacy and Security Officer (IPSO) or relevant staff to ensure that a secure method is being used. The Data Exchange Gateway is the preferred method of providing data to third-party administrators or other non-state partners. If not a feasible alternative, alternative methods that may be acceptable, with the prior approval of the IPSO, may include:

- Establishing a State e-mail account for the intended recipient
- Encrypting a file containing the confidential or restricted data and sending the encrypted file and password in separate communications
- Secured file transfer protocol services
- Other commercial solutions that DTMB Enterprise Architecture can evaluate

	Effective Date:	09-12-2011	
	Policy #:	G-19	
	Supersedes:		
Subject: Information Privacy and Security Encryption		Page:	2 of 2

ENFORCEMENT

All department staff must report suspected violations of this policy to the appropriate supervisor and the IPSO. Violations of this policy, including the failure to report one's own improper transmission of confidential or restricted data, are grounds for discipline, up to and including dismissal.