

	Effective Date:	10-01-2015
	Policy #:	G-38
	Supersedes:	
Subject: Data Classification	Page:	Page 1 of 4

PURPOSE

Provide a framework to protect Department of Licensing and Regulatory Affairs (LARA) data from security compromises that involve misuse, unauthorized access, disclosure, modification, or deletion which could cause:

- Loss of revenue
- Violation of statutory requirements
- Violation of contractual agreements
- Compromise of customer privacy
- Identity theft
- Untimely and inefficient customer service

This document establishes LARA’s policy regarding how LARA’s data should be classified, regardless of the medium on which it is stored in accordance with DTMB Cybersecurity and Infrastructure Protection (CIP) and DTMB Data Classification Standard 1340.00.14 and 1340.00.14.01.

SCOPE

This policy applies to employees, contractors, consultants, temporary employees, trusted partners, personnel affiliated with third parties or vendors, and all other workers affiliated with LARA who use LARA’s information network and IT resources. All of these sources are referred to in the rest of this document as “personnel.” This policy applies to any format of data including paper, email, video, media device, electronic, information systems, etc.

POLICY

LARA’s Data Manager and Chief Data Steward will be responsible, in conjunction with LARA Data Owners, for determining the appropriate security classifications for data. This determination will include:

- Identifying who may perform changes to the data, and under what conditions
- Identifying the sensitivity of the data

	Effective Date:	10-01-2015	
	Policy #:	G-38	
	Supersedes:		
Subject: Data Classification		Page:	Page 2 of 4

- Communicating the classification and details to custodians, contractors, users, and recipients.

The data manager/chief data steward/owners are responsible for coordinating with the Department of Technology, Management and Budget (DTMB) personnel to ensure that information security needs are met.

Only the data manager/owner may downgrade or declassify data.

- Downgrading is the process of reclassifying data to a less restricted level of security.
- Declassifying is the process of reclassifying data from “non-public” to “public.”

All bureaus/agencies within LARA are required to comply with this policy and DTMB standard and procedure:

[1340.00.14 Information Technology Information Security Data Classification](#)

And

[1340.00.14.01 Instructions for Completion of Data Classification Forms](#)

Data Classification Levels attached.

	Effective Date:	10-01-2015
	Policy #:	G-38
	Supersedes:	
Subject: Data Classification		Page: Page 3 of 4

Data Classification Levels		
Data Classification Level	Description	Examples
Public	Public data is information that has been explicitly approved for distribution to the public and can be disclosed to anyone without violating an individual's right to privacy or causing any potential harm. Public data is not sensitive in context or content and does not require special protection. If disclosed or compromised, it will not expose the SOM to financial loss or embarrassment, compromise a competitive advantage, or jeopardize the security information.	<ul style="list-style-type: none"> • Agency Public Website • Brochures or News Releases • Publicly Available Financial Reports • Executive Budgets • Non-Exempt FOIA Documents
Internal	Internal data is information that is not sensitive to disclosure within the agency. By default, data created, updated or stored by the Agency is considered to be Internal information intended for use by agency employees and authorized non-agency employees, although it may be accessed by trusted partners covered by a non-disclosure agreement. This information shall be shared internally to further internal operations, lower costs, prevent duplication, and otherwise enhance the condition or operation of Agency systems.	<ul style="list-style-type: none"> • Agency Policies and Procedures • Customer Information • Driver History Records • Internal Announcements and Communications • Internal Phone Directories and Organizational Charts • Network Diagrams • Non-sensitive Operational Reports



Effective Date:

10-01-2015

Policy #:

G-38

Supersedes:

Subject:

Data Classification

Page:

Page 4 of 4

<p>Confidential</p>	<p>Confidential data is sensitive information wherein unauthorized disclosure could cause serious financial, legal, or reputational damage to an agency or the SOM. Confidential data may include personal identifying information (PII) or confidential non-public information that relates to an agency's business. Confidential data should only be made available to authorized personnel on a need-to-know basis and should require a signed non-disclosure agreement.</p>	<ul style="list-style-type: none"> • Social Security Numbers • Credit Card Numbers • Civil Investigative Data • Criminal History Data • Confidential Business Information • Financial Statements • Health and Medical Records • Configuration and Architecture of the SOM Internal Network
----------------------------	---	--

<p>Restricted</p>	<p>Restricted data is information that is extremely sensitive and any disclosure or corruption could be hazardous to life or health, cause extreme damage to integrity or image, and/or impair the effective delivery of services. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact. Restricted data can be made available to named individuals or specific positions on a need-to-know basis.</p>	<ul style="list-style-type: none"> • Sensitive Law Enforcement Data • Investigative Records and Communications Systems • Disaster Recovery and Business Continuity Plans
--------------------------	--	---