D4 Data and Ethics

Autumn 2022 | Lecture 3 - Part III

Focus: Information security & cybersecurity | Author: Prof. Dr. Petra Maria Asprion | FHNW

© Picture Raphael Stöckli, MT cover 2018

Agenda

Part I -- Repetition L1 → SD1

Part II -- Organization Layer: Relevant References → SD2

Part III -- Organization Layer: First control - IS Policy → SD3

Part IV -- Organization Layer: Selective control - GEIGER → SD4

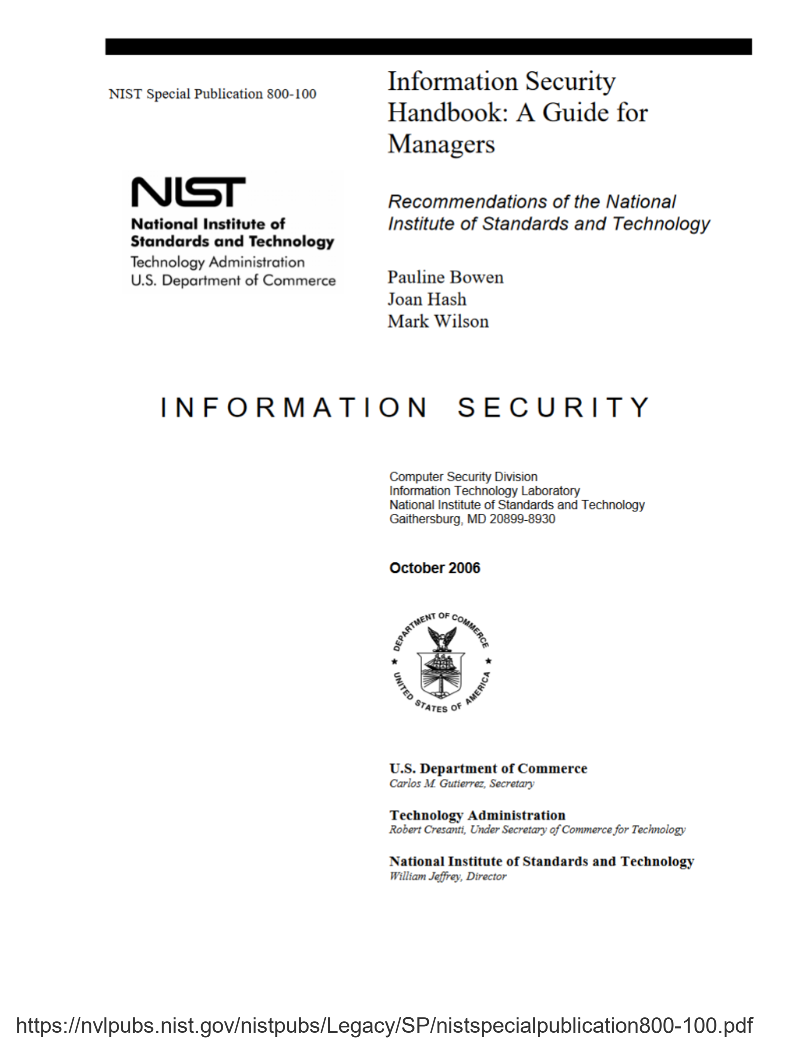
Coaching Session #3 → SD5

→ SD = Slide Deck

Information Security Handbook

SP 800-100 (2007)

A holistic approach to manage Information Security



NIST Special Publication 800-100

Information Security Handbook: A Guide for Managers

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Recommendations of the National Institute of Standards and Technology

Pauline Bowen
Joan Hash
Mark Wilson

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

The NIST 800 series is a technical standard set of publications that details U.S. government procedures, policies, and guidelines on information systems - developed by the National Institute of Standards and Technology

Have a look (related website):
https://csrc.nist.gov/publications/detail/sp/800-100/final

Information Security Handbook

SP 800-100 (2007)

A holistic approach to manage Information Security

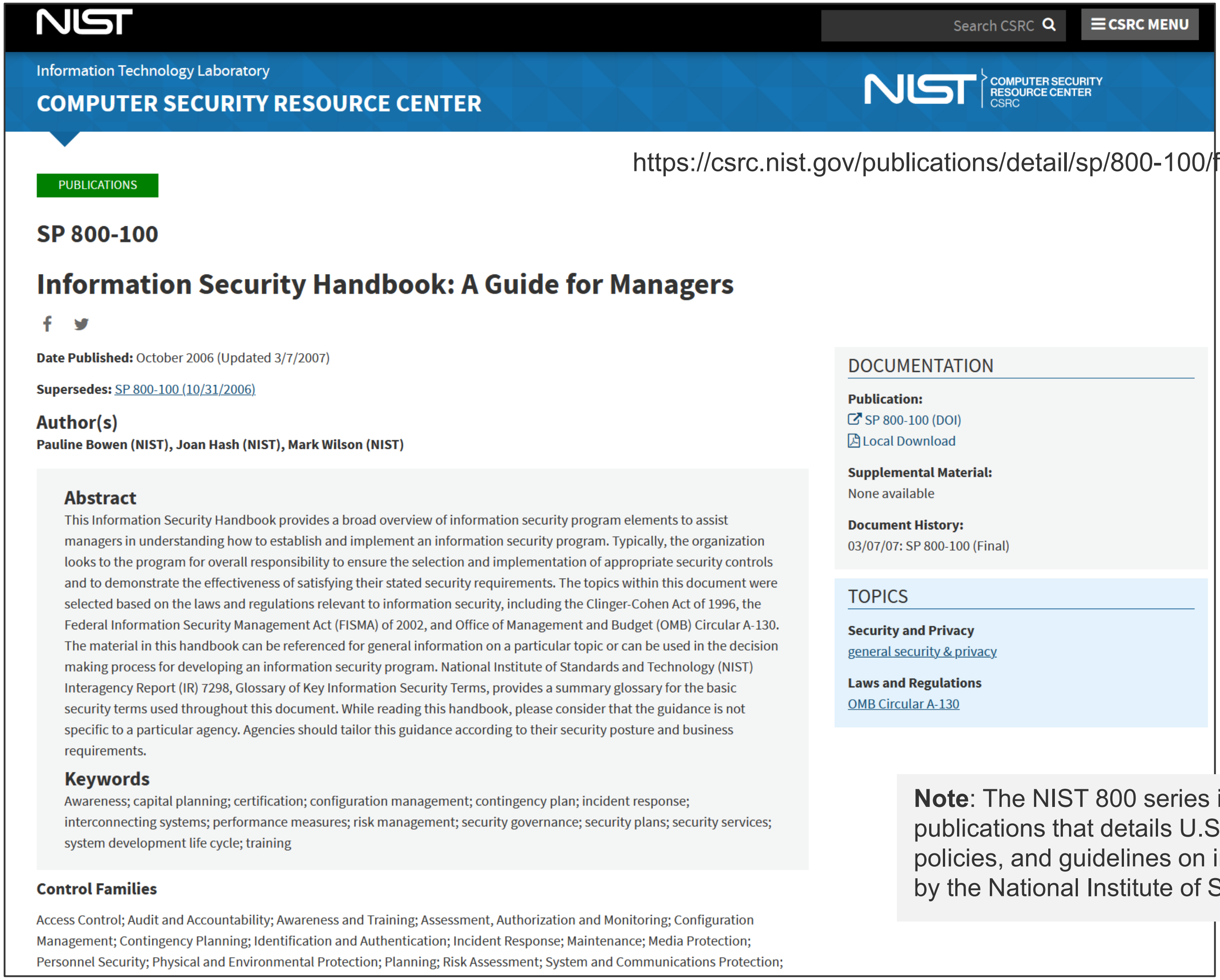
This Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Typically, the organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements. […] **The material in this handbook can be referenced for general information on a particular topic or can be used in the decision making process for developing an information security program**.

Control Families

Access Control; Audit and Accountability; Awareness and Training; Assessment, Authorization and Monitoring; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Personnel Security; Physical and Environmental Protection; Planning; Risk Assessment; System and Communications Protection; System and Information Integrity; System and Services Acquisition

Information Security Handbook:

Guide for Managers -- SP 800-100 (2007)



NIST
Search CSRC
☰ CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
PUBLICATIONS

https://csrc.nist.gov/publications/detail/sp/800-100/final

SP 800-100

Information Security Handbook: A Guide for Managers

Date Published: October 2006 (Updated 3/7/2007)

Supersedes: SP 800-100 (10/31/2006)

Author(s)

Pauline Bowen (NIST), Joan Hash (NIST), Mark Wilson (NIST)

Abstract

This Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Typically, the organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements. The topics within this document were selected based on the laws and regulations relevant to information security, including the Clinger-Cohen Act of 1996, the Federal Information Security Management Act (FISMA) of 2002, and Office of Management and Budget (OMB) Circular A-130. The material in this handbook can be referenced for general information on a particular topic or can be used in the decision making process for developing an information security program. National Institute of Standards and Technology (NIST) Interagency Report (IR) 7298, Glossary of Key Information Security Terms, provides a summary glossary for the basic security terms used throughout this document. While reading this handbook, please consider that the guidance is not specific to a particular agency. Agencies should tailor this guidance according to their security posture and business requirements.

Keywords

Awareness; capital planning; certification; configuration management; contingency plan; incident response; interconnecting systems; performance measures; risk management; security governance; security plans; security services; system development life cycle; training

Control Families

Access Control; Audit and Accountability; Awareness and Training; Assessment, Authorization and Monitoring; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Personnel Security; Physical and Environmental Protection; Planning; Risk Assessment; System and Communications Protection;

DOCUMENTATION

Publication:
SP 800-100 (DOI)
Local Download

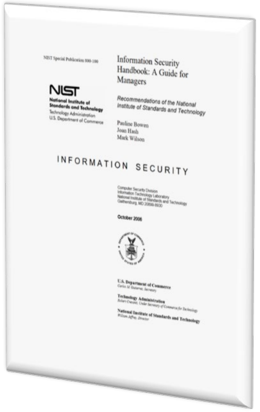
Supplemental Material:
None available

Document History:
03/07/07: SP 800-100 (Final)

TOPICS

Security and Privacy
general security & privacy

Laws and Regulations
OMB Circular A-130



NIST Special Publication 800-100

Information Security Handbook: A Guide for Managers

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Recommendations of the National Institute of Standards and Technology

Pauline Bowen
Joan Hash
Mark Wilson

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Note: The NIST 800 series is a technical standard set of publications that details U.S. government procedures, policies, and guidelines on information systems - developed by the National Institute of Standards and Technology.

Information Security Handbook:

SP 800-100 (2007) – Main Areas

The Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program.

Chapter 1: Introduction

Excerpt see next slide

Chapter 2: Information Security Governance

Chapter 3: System Development Life Cycle

Chapter 4: Awareness and Training

Chapter 5: Capital Planning and Investment Control

Chapter 6: Interconnecting Systems

Chapter 7: Performance Measures

Chapter 8: Security Planning

Chapter 9: Information Technology Contingency Planning

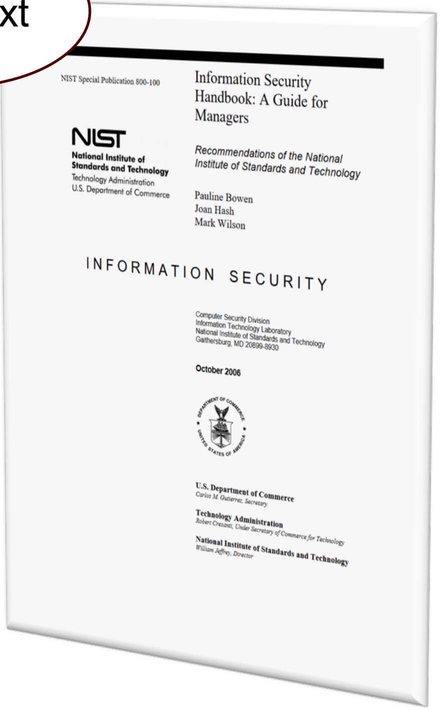
Chapter 10: Risk Management

Chapter 11: Certification, Accreditation, and Security Assessments

Chapter 12: Security Services and Products Acquisition

Chapter 13: Incident Response

Chapter 14: Configuration Management



NIST Special Publication 800-100

Information Security Handbook: A Guide for Managers

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Recommendations of the National Institute of Standards and Technology

Pauline Bowen
Joan Hash
Mark Wilson

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

Information Security Handbook:

SP 800-100 (2007) – Chapter 2.2.5 (Excerpt)

Chapter 2: Information Security Governance –
2.2.5 Information Security Policy and Guidance

Information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information security policy is an essential component of information security governance — without the policy, governance has no substance and rules to enforce.

Information security policy should be based on a combination of appropriate legislation, such as FISMA; applicable standards, such as NIST Federal Information Processing Standards (FIPS)* and guidance; and internal agency requirements.

Agency information security policy should address the fundamentals of agency information security governance structure, including:

- Information security roles and responsibilities;
- Statement of security controls baseline and rules for exceeding the baseline; and
- Rules of behavior that agency users are expected to follow and minimum repercussions for noncompliance.

[…]

* See next slide

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

Information Security Handbook:

SP 800-100 (2007) – Chapter 2.2.5 (Excerpt)

Chapter 8: Security Planning –

8.5 Security Control Selection

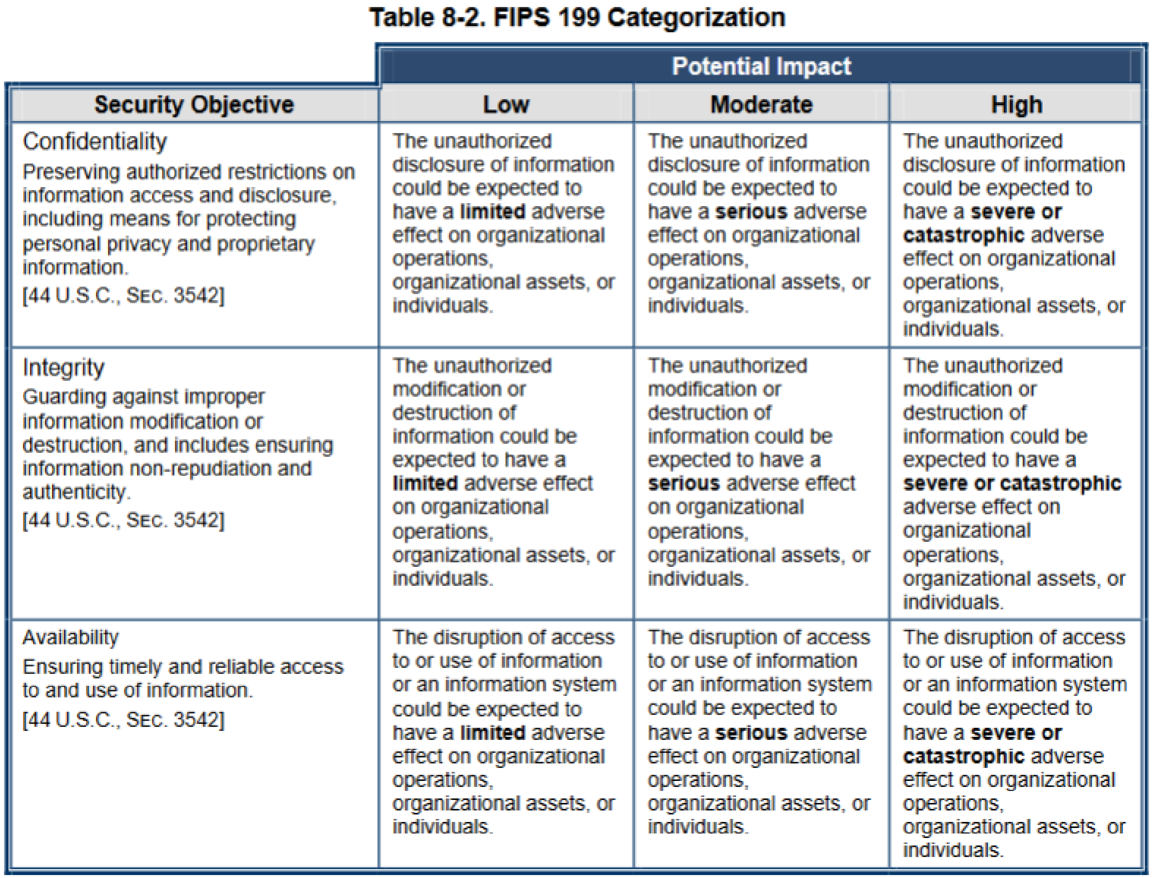


Table 8-2. FIPS 199 Categorization

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

FIPS 199 -- NIST Standards for Security Categorization of Federal Information and Information Systems https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

Excerpt see
Information Security Handbook:
A Guide for Managers
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf | page 75

A practical Example

Information Security Policy

Reminder

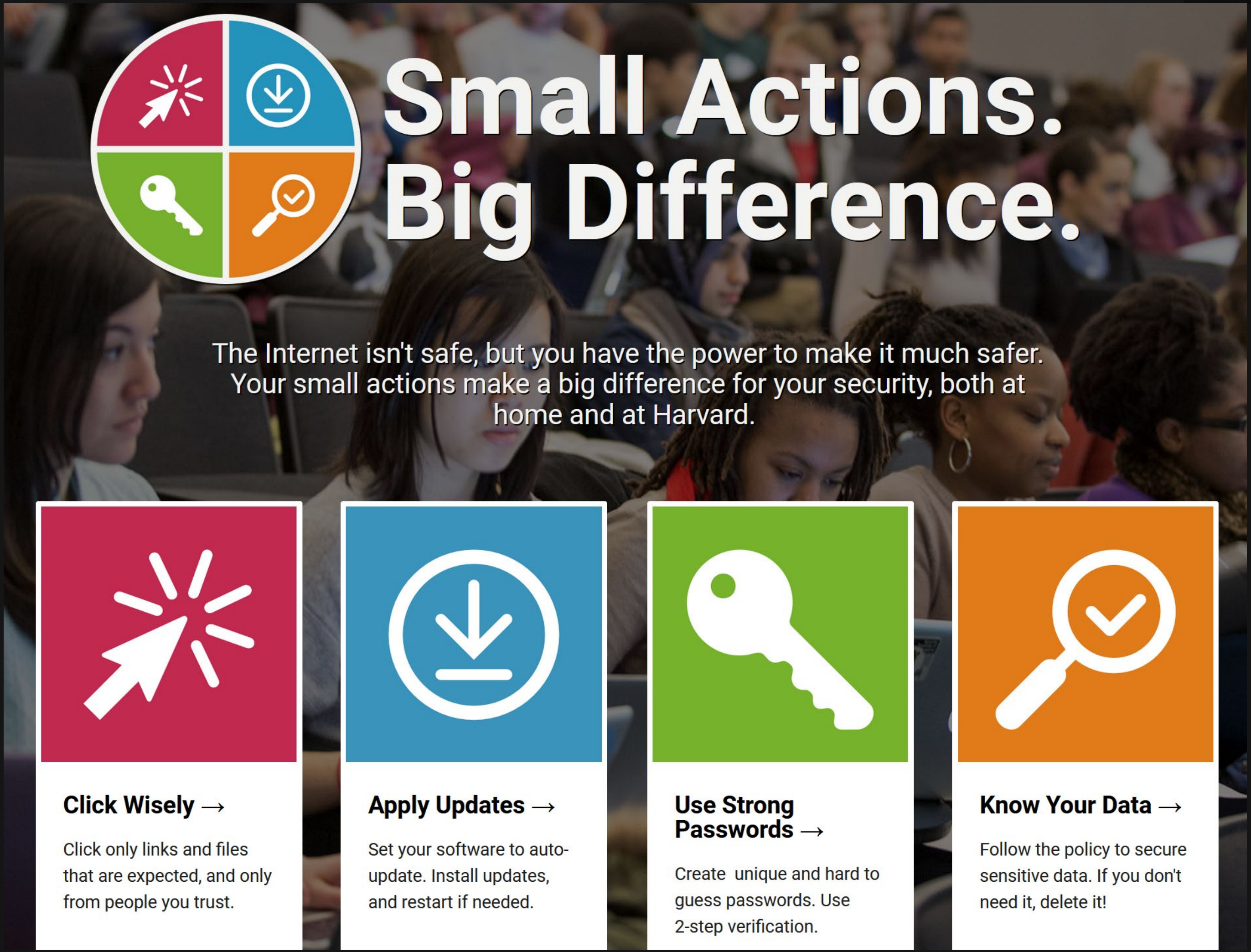
Information Security Policy --

Definition

> "*Information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information*"

NIST SP 800-53, Revision 1, 'Recommended Security Controls for Federal Information Systems,' 2006

Example from Harvard University



Small Actions. Big Difference.

The Internet isn't safe, but you have the power to make it much safer. Your small actions make a big difference for your security, both at home and at Harvard.

Click Wisely →

Click only links and files that are expected, and only from people you trust.

Apply Updates →

Set your software to auto-update. Install updates, and restart if needed.

Use Strong Passwords →

Create unique and hard to guess passwords. Use 2-step verification.

Know Your Data →

Follow the policy to secure sensitive data. If you don't need it, delete it!

Harvard University -- https://security.harvard.edu/

Information Security Policy --
Example -- Harvard University

Policy Statements I/III

Harvard University is committed to protecting the information that is critical to teaching, research, and the University's many varied activities, our business operation, and the communities we support, including students, faculty, staff members, and the public. These protections may be governed by legal, contractual, or University policy considerations.

Everyone at Harvard has a responsibility for proper handling and protection of Harvard confidential information and Harvard systems as set out in the Policy Statements. These policies apply to the entire Harvard community including faculty, staff, and students. Each policy is supported by Requirements that describe what must be done to be in compliance. Specific implementation steps are described in the How-Tos that accompany the Requirements.

"Harvard confidential information" refers to non-public information of any level that Harvard manages directly or via contract. "Harvard systems" means Harvard-owned, Harvard-purchased, or Harvard-managed systems, whether on Harvard premises or through contracted Cloud-based service.

For questions about policy interpretation, assistance with implementation steps or to find out about information security services that are offered at Harvard, contact xxx@harvard.edu.

Harvard is equally committed to preserving an environment that encourages academic and research collaboration through the responsible use of information technology resources. Find out about the Harvard Research Data Security Policy (HRDSP) and associated guidance in support of Harvard's research mission.

Adopted from Harvard University -- https://policy.security.harvard.edu/policies

Information Security Policy --

Example -- Harvard University

Policy Statements II/III

1. All users are responsible for protecting Harvard confidential information that they use in any form from unauthorized access and use.
2. All users are responsible for protecting their Harvard passwords and other access credentials from unauthorized use.
3. All access to and use of Harvard confidential information must be for authorized Harvard purposes.
4. Harvard systems must not be used in a manner that violates University policies.
5. All persons accessing Harvard confidential information must be trained in protecting such information.
6. All users of Harvard confidential information resources must be accurately and individually identified.
7. Harvard confidential information must be protected on any computer or device.
8. All Harvard systems and systems storing Harvard confidential information must be protected against improper access.
9. All critical systems, and systems and locations where Level 4 or 5 information is stored, must be accurately identified and physically secure.
10. Electronic and physical records containing Harvard confidential information must be appropriately protected when transported or transmitted.
11. Software must be kept up to date on all Harvard systems and systems storing Harvard confidential information.
12. Electronic and physical records containing Harvard confidential information must be properly disposed of so that the information cannot be retrieved or reassembled when no longer needed or required to be kept.
13. Harvard must conduct appropriate due diligence on third parties that will store or have access to Harvard confidential information or sensitive systems.
14. Any actual or suspected loss, theft, or improper use of or access to, Harvard confidential information or systems must be reported **

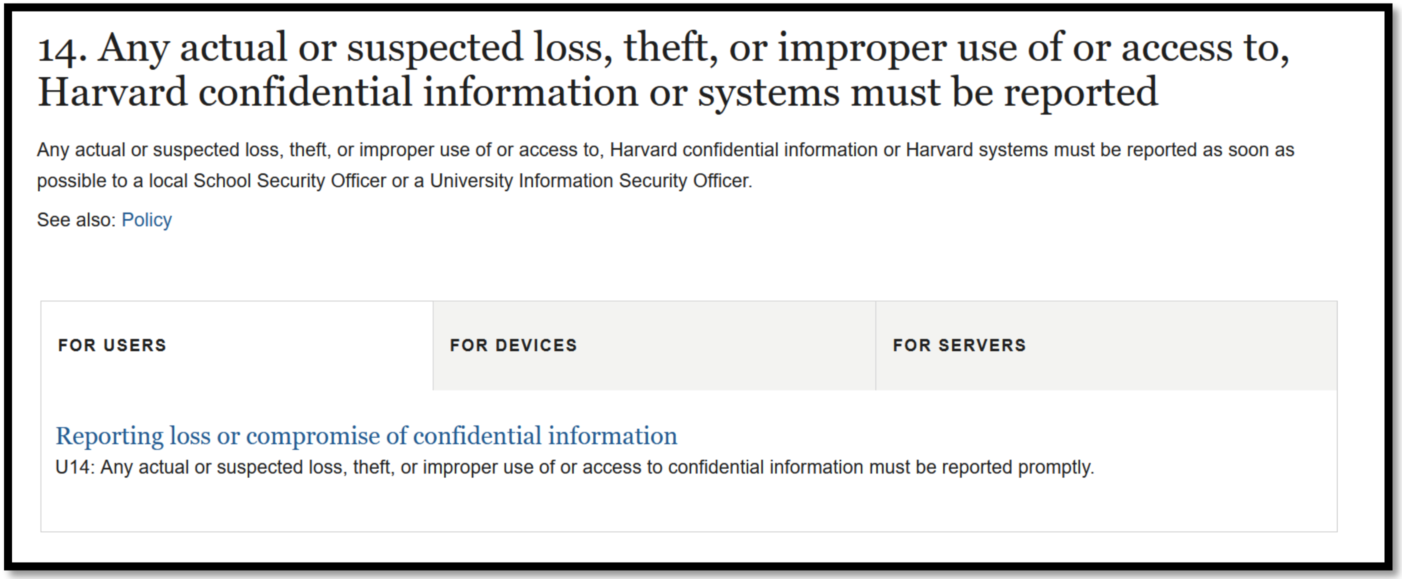
Note: Each statement is linked to additional information.
** see next slide

Adopted from Harvard University -- https://policy.security.harvard.edu/policies

Information Security Policy --
Example -- Harvard University

Policy Statements III/III

14. Any actual or suspected loss, theft, or improper use of or access to, Harvard confidential information or systems must be reported **



14. Any actual or suspected loss, theft, or improper use of or access to, Harvard confidential information or systems must be reported

Any actual or suspected loss, theft, or improper use of or access to, Harvard confidential information or Harvard systems must be reported as soon as possible to a local School Security Officer or a University Information Security Officer.

See also: Policy

FOR USERS	FOR DEVICES	FOR SERVERS

Reporting loss or compromise of confidential information

U14: Any actual or suspected loss, theft, or improper use of or access to confidential information must be reported promptly.

Adopted from Harvard University -- https://policy.security.harvard.edu/policies

Information Security Policy

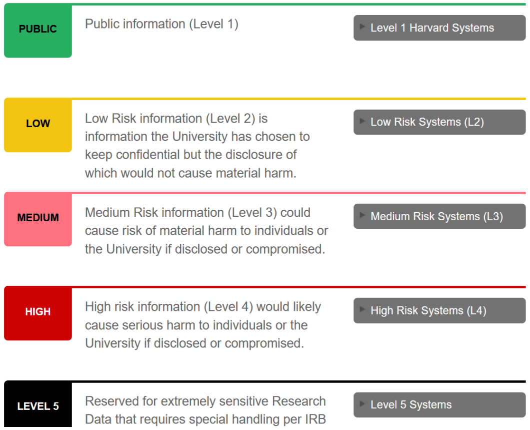
Information Security Policy --
Example -- Harvard University

Introduction

The Information Security Policy consists of three elements:
Policy Statements | Requirements | How To’s

Choose a Security Control level below to view associated Requirements based on the higher of the two, data risk level* or system risk level. The higher the level, the greater the required protection.

- All non-public information that Harvard manages directly or via contract is defined as "Harvard confidential information."
- "Harvard systems" means Harvard-owned or Harvard-managed systems, whether on Harvard premises or through contracted Cloud-based service.

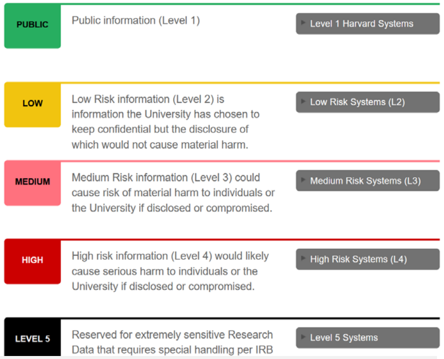


PUBLIC	Public information (Level 1)	Level 1 Harvard Systems
LOW	Low Risk information (Level 2) is information the University has chosen to keep confidential but the disclosure of which would not cause material harm.	Low Risk Systems (L2)
MEDIUM	Medium Risk information (Level 3) could cause risk of material harm to individuals or the University if disclosed or compromised.	Medium Risk Systems (L3)
HIGH	High risk information (Level 4) would likely cause serious harm to individuals or the University if disclosed or compromised.	High Risk Systems (L4)
LEVEL 5	Reserved for extremely sensitive Research Data that requires special handling per IRB	Level 5 Systems

* see the five levels incl. examples on the next slides

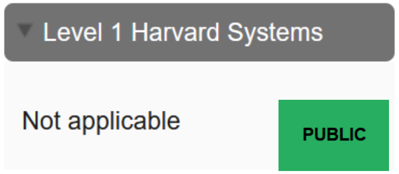
Adopted from Harvard University -- https://policy.security.harvard.edu/

Information Security Policy --
Example -- Harvard University



PUBLIC	Public information (Level 1)	Level 1 Harvard Systems
LOW	Low Risk information (Level 2) is information the University has chosen to keep confidential but the disclosure of which would not cause material harm.	Low Risk Systems (L2)
MEDIUM	Medium Risk information (Level 3) could cause risk of material harm to individuals or the University if disclosed or compromised.	Medium Risk Systems (L3)
HIGH	High risk information (Level 4) would likely cause serious harm to individuals or the University if disclosed or compromised.	High Risk Systems (L4)
LEVEL 5	Reserved for extremely sensitive Research Data that requires special handling per IRB	Level 5 Systems

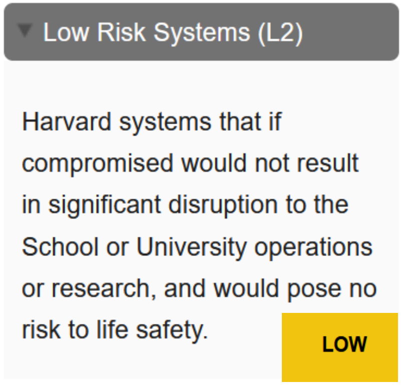
Data Risk Level -- Classification Levels



Level 1 Harvard Systems

Not applicable

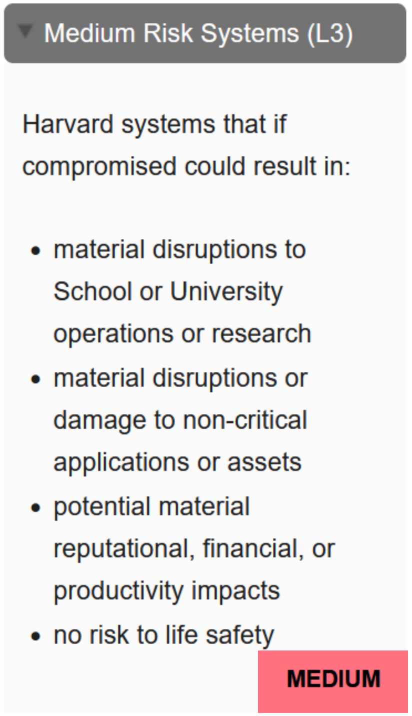
PUBLIC



Low Risk Systems (L2)

Harvard systems that if compromised would not result in significant disruption to the School or University operations or research, and would pose no risk to life safety.

LOW

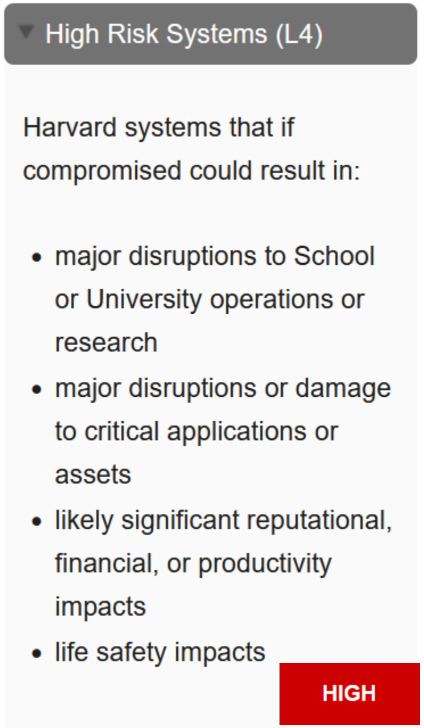


Medium Risk Systems (L3)

Harvard systems that if compromised could result in:

- material disruptions to School or University operations or research
- material disruptions or damage to non-critical applications or assets
- potential material reputational, financial, or productivity impacts
- no risk to life safety

MEDIUM

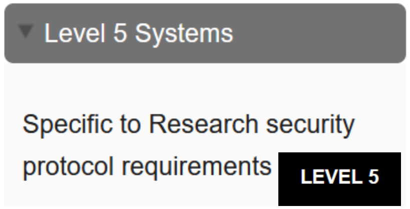


High Risk Systems (L4)

Harvard systems that if compromised could result in:

- major disruptions to School or University operations or research
- major disruptions or damage to critical applications or assets
- likely significant reputational, financial, or productivity impacts
- life safety impacts

HIGH



Level 5 Systems

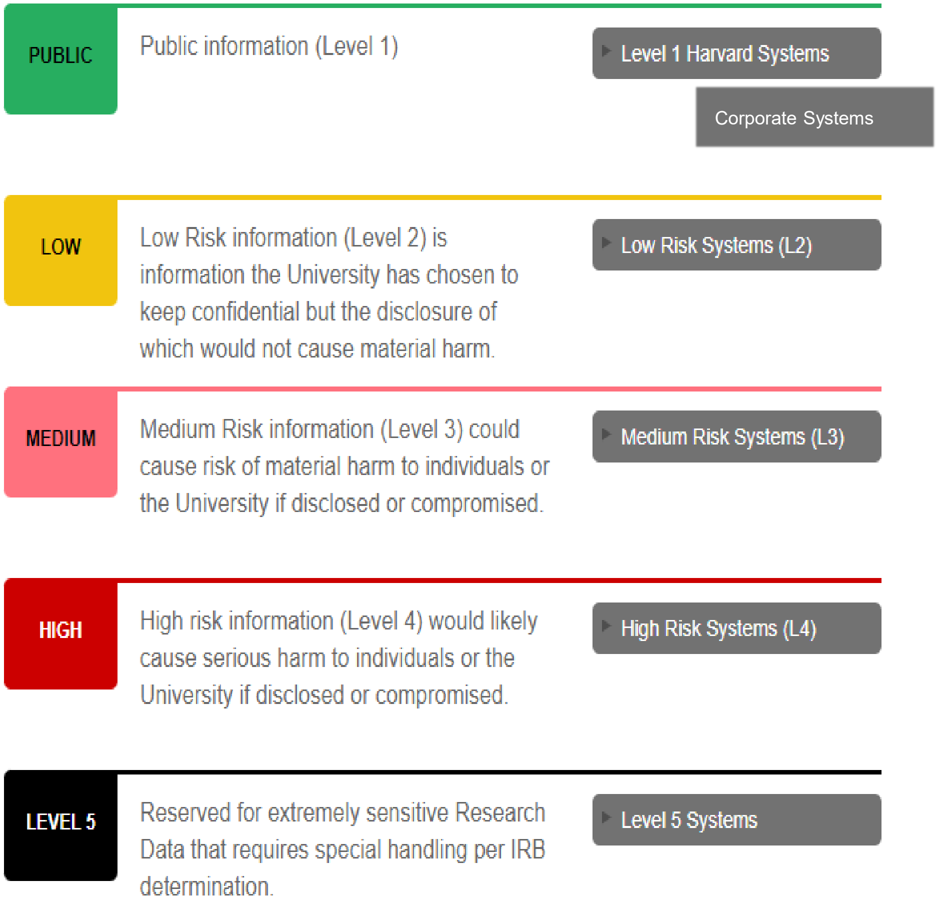
Specific to Research security protocol requirements

LEVEL 5

* see next slide

Adopted from Harvard University -- https://policy.security.harvard.edu/

Information Security Policy -- Content



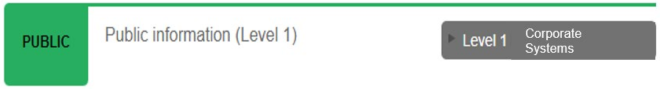
PUBLIC	Public information (Level 1)	Level 1 Harvard Systems Corporate Systems
LOW	Low Risk information (Level 2) is information the University has chosen to keep confidential but the disclosure of which would not cause material harm.	Low Risk Systems (L2)
MEDIUM	Medium Risk information (Level 3) could cause risk of material harm to individuals or the University if disclosed or compromised.	Medium Risk Systems (L3)
HIGH	High risk information (Level 4) would likely cause serious harm to individuals or the University if disclosed or compromised.	High Risk Systems (L4)
LEVEL 5	Reserved for extremely sensitive Research Data that requires special handling per IRB determination.	Level 5 Systems

On the following slides a data classification is listed, as it can also be operated by a university

Adopted from Harvard University -- https://policy.security.harvard.edu/

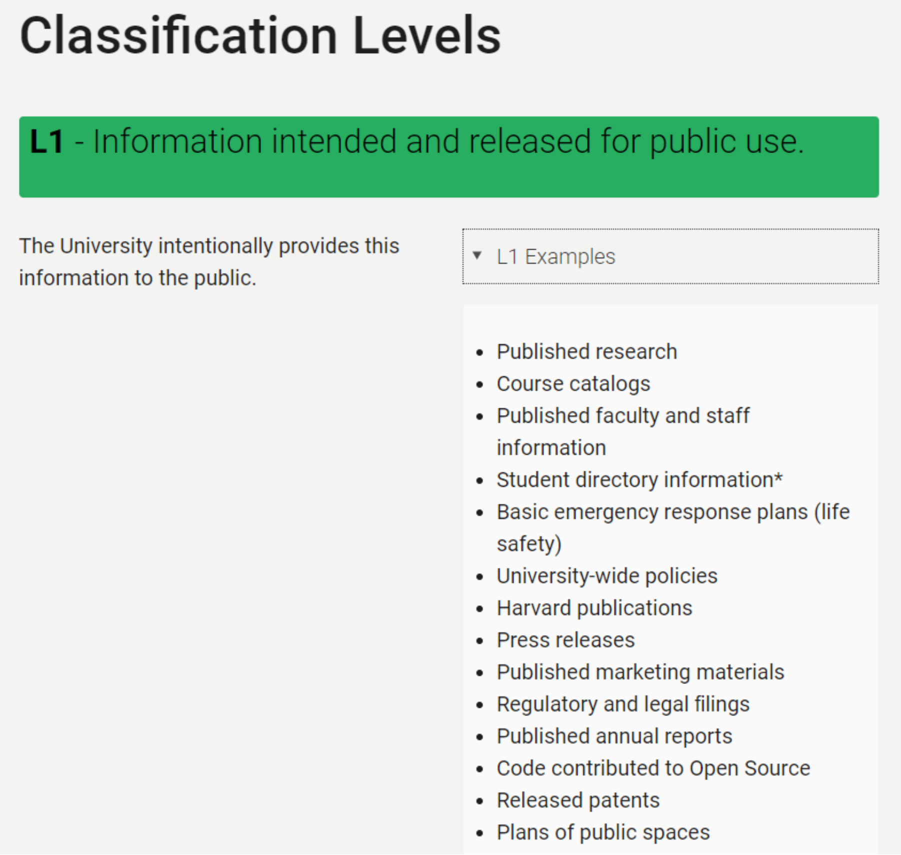
Information Security Policy --

Data Classification



PUBLIC

Public information (Level 1)



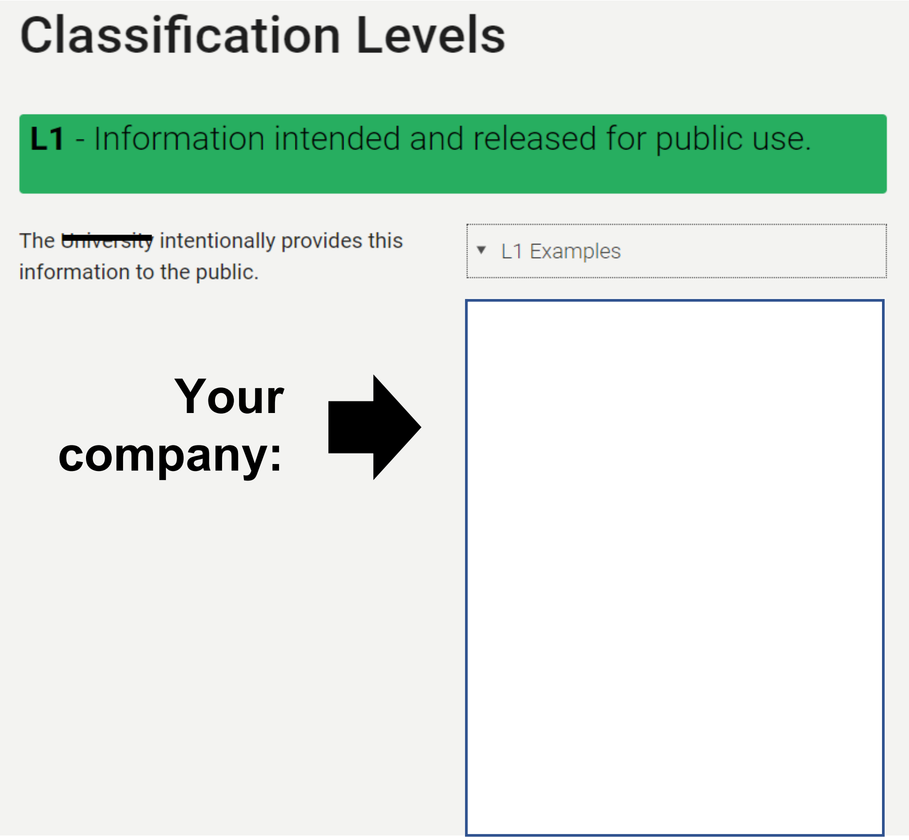
Classification Levels

L1 - Information intended and released for public use.

The University intentionally provides this information to the public.

▾ L1 Examples

- Published research
- Course catalogs
- Published faculty and staff information
- Student directory information*
- Basic emergency response plans (life safety)
- University-wide policies
- Harvard publications
- Press releases
- Published marketing materials
- Regulatory and legal filings
- Published annual reports
- Code contributed to Open Source
- Released patents
- Plans of public spaces



Classification Levels

L1 - Information intended and released for public use.

The ~~University~~ intentionally provides this information to the public.

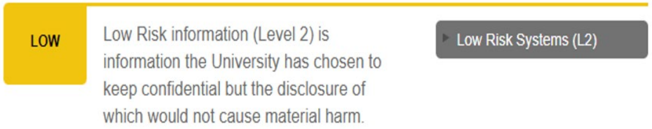
▾ L1 Examples

Your company:

Adopted from Harvard University -- https://policy.security.harvard.edu/

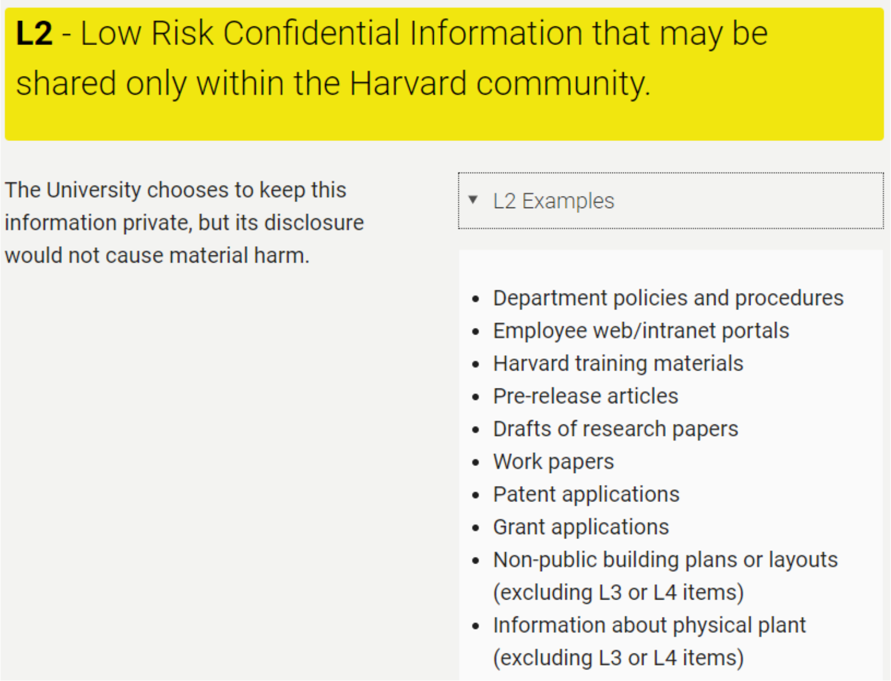
Information Security Policy --

Data Classification



LOW

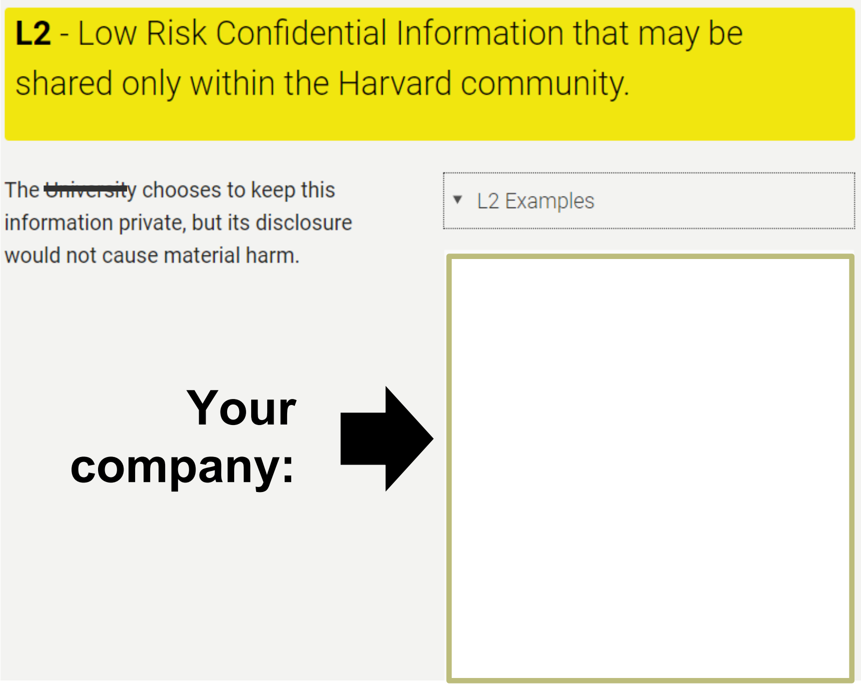
Low Risk information (Level 2) is information the University has chosen to keep confidential but the disclosure of which would not cause material harm.



L2 - Low Risk Confidential Information that may be shared only within the Harvard community.

The University chooses to keep this information private, but its disclosure would not cause material harm.

- Department policies and procedures
- Employee web/intranet portals
- Harvard training materials
- Pre-release articles
- Drafts of research papers
- Work papers
- Patent applications
- Grant applications
- Non-public building plans or layouts (excluding L3 or L4 items)
- Information about physical plant (excluding L3 or L4 items)



L2 - Low Risk Confidential Information that may be shared only within the Harvard community.

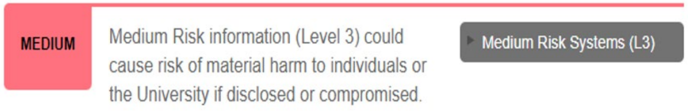
The ~~University~~ chooses to keep this information private, but its disclosure would not cause material harm.

Your company:

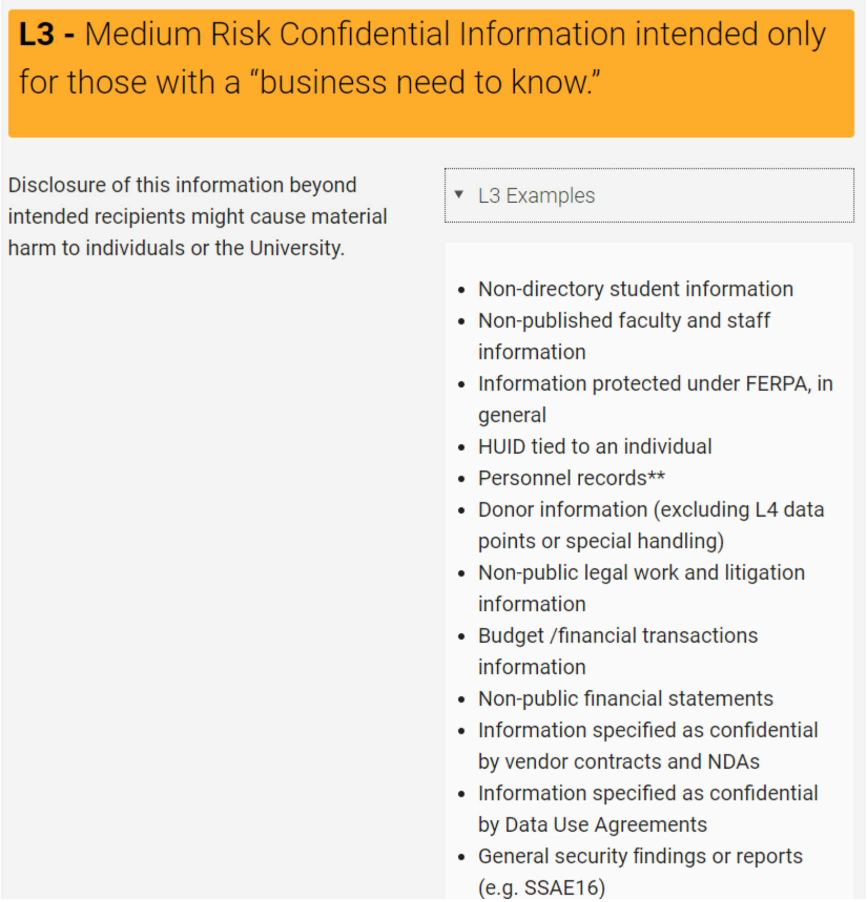
Adopted from Harvard University -- https://policy.security.harvard.edu/

Information Security Policy

Information Security Policy --
Data Classification

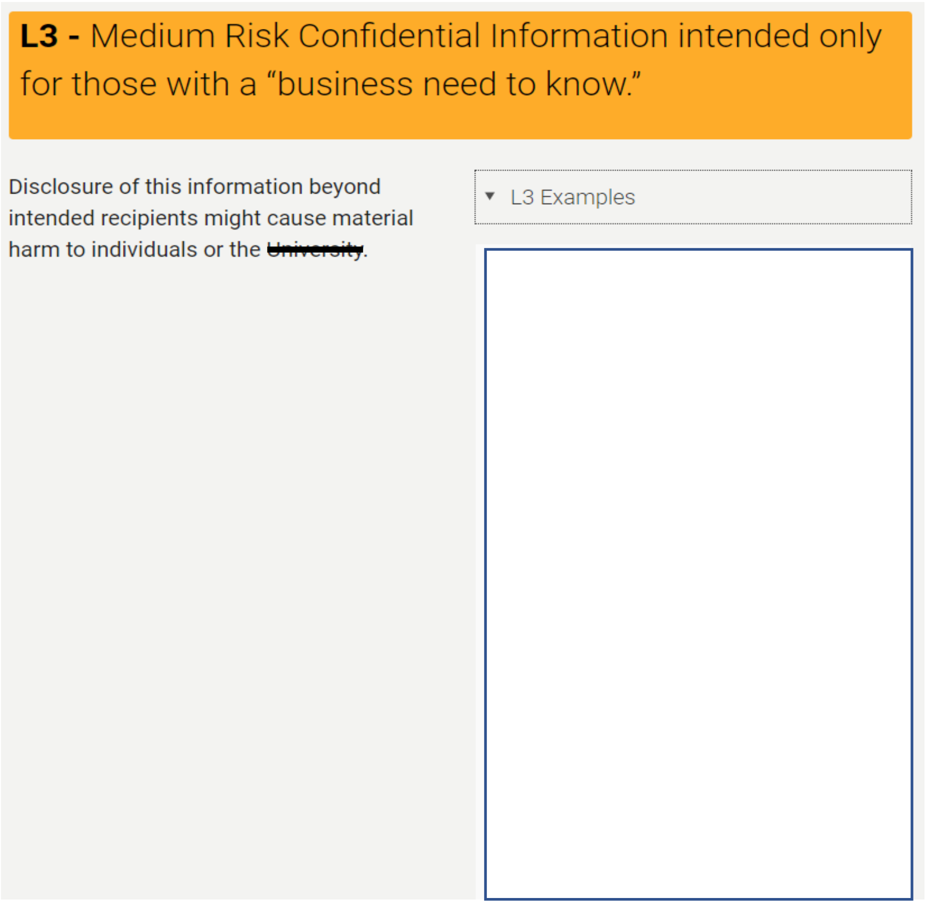


Medium Risk information (Level 3) could cause risk of material harm to individuals or the University if disclosed or compromised.


L3 - Medium Risk Confidential Information intended only for those with a "business need to know."

Disclosure of this information beyond intended recipients might cause material harm to individuals or the University.

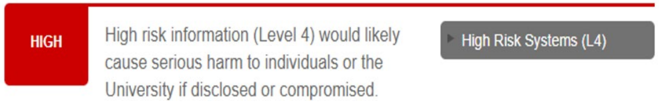
- Non-directory student information
- Non-published faculty and staff information
- Information protected under FERPA, in general
- HUID tied to an individual
- Personnel records**
- Donor information (excluding L4 data points or special handling)
- Non-public legal work and litigation information
- Budget /financial transactions information
- Non-public financial statements
- Information specified as confidential by vendor contracts and NDAs
- Information specified as confidential by Data Use Agreements
- General security findings or reports (e.g. SSAE16)


L3 - Medium Risk Confidential Information intended only for those with a "business need to know."

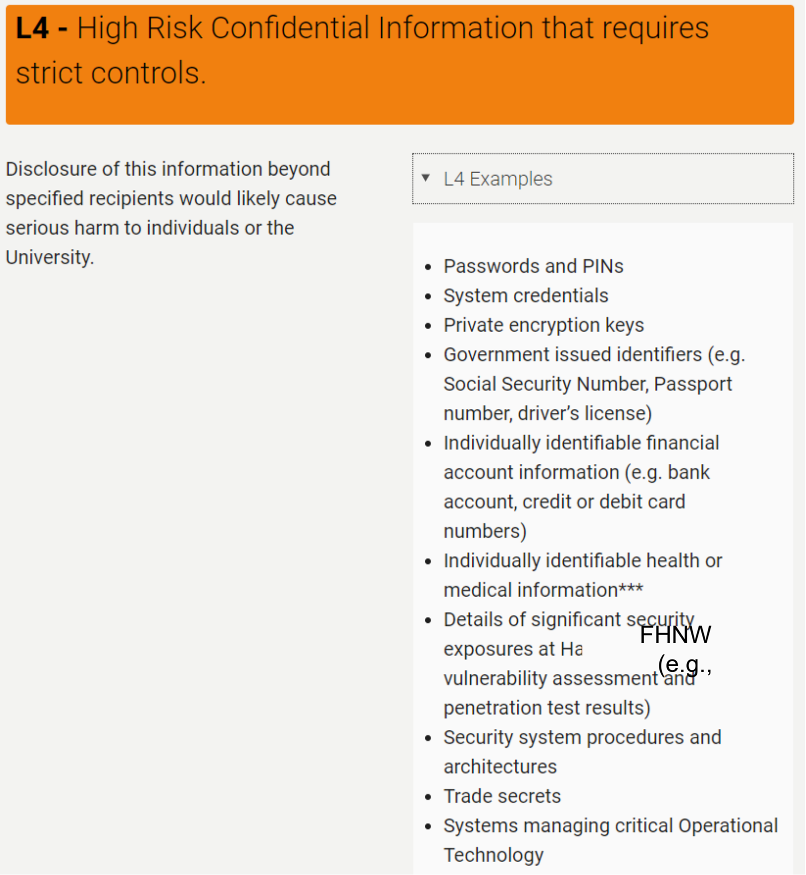
Disclosure of this information beyond intended recipients might cause material harm to individuals or the ~~University~~.

Adopted from Harvard University -- https://policy.security.harvard.edu/

Information Security Policy --
Data Classification

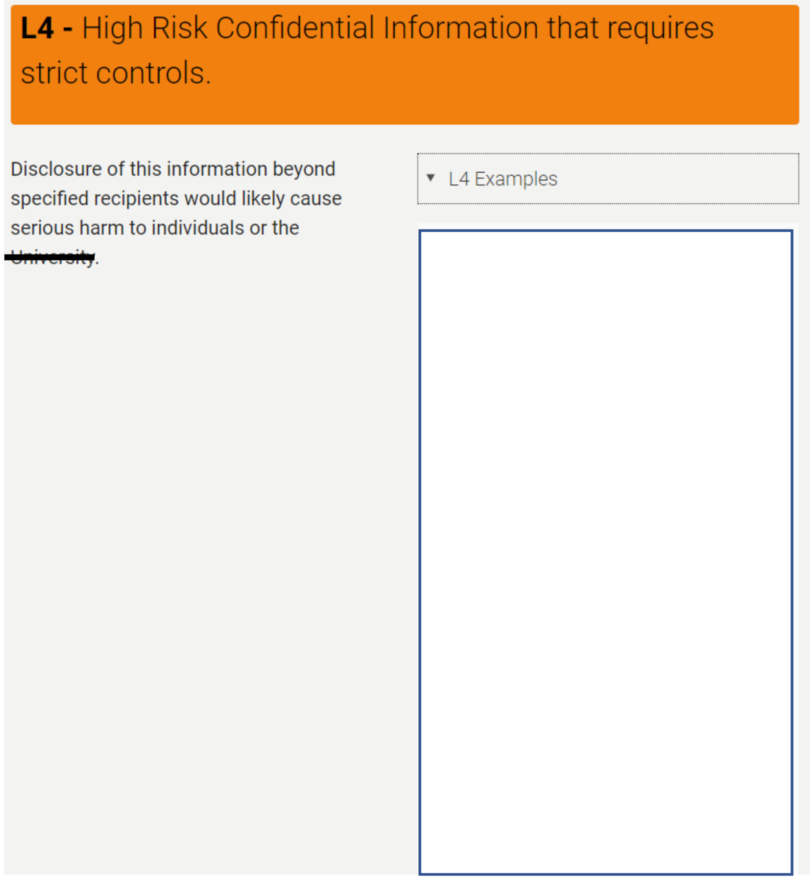

HIGH

High risk information (Level 4) would likely cause serious harm to individuals or the University if disclosed or compromised.


L4 - High Risk Confidential Information that requires strict controls.

Disclosure of this information beyond specified recipients would likely cause serious harm to individuals or the University.

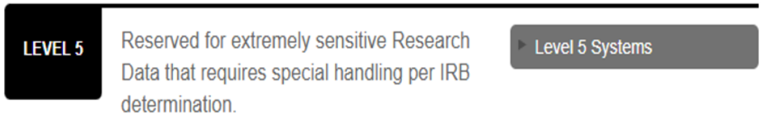
- Passwords and PINs
- System credentials
- Private encryption keys
- Government issued identifiers (e.g. Social Security Number, Passport number, driver's license)
- Individually identifiable financial account information (e.g. bank account, credit or debit card numbers)
- Individually identifiable health or medical information***
- Details of significant security exposures at Ha FHNW (e.g., vulnerability assessment and penetration test results)
- Security system procedures and architectures
- Trade secrets
- Systems managing critical Operational Technology


L4 - High Risk Confidential Information that requires strict controls.

Disclosure of this information beyond specified recipients would likely cause serious harm to individuals or the ~~University~~.

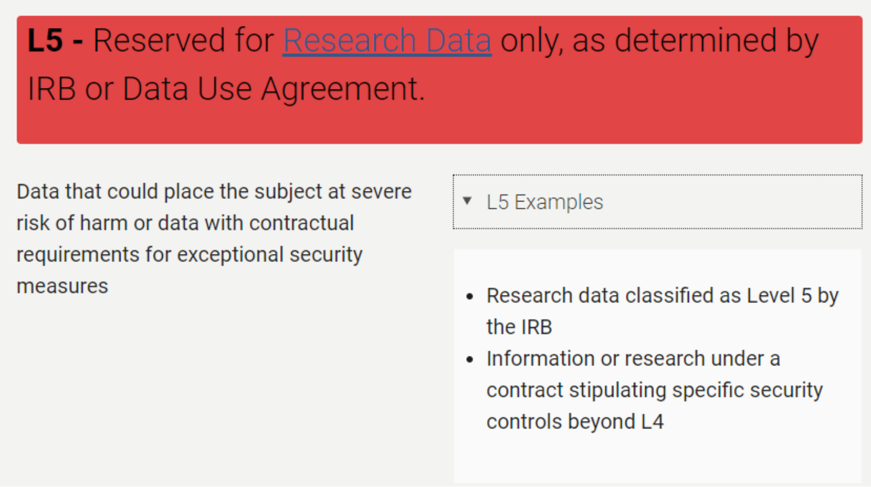
Adopted from Harvard University -- https://policy.security.harvard.edu/

Information Security Policy -- Data Classification



LEVEL 5

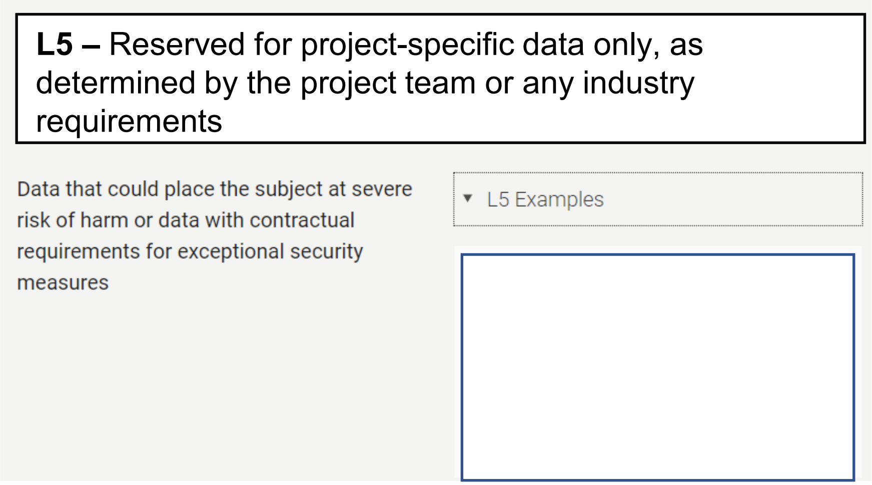
Reserved for extremely sensitive Research Data that requires special handling per IRB determination.



L5 - Reserved for Research Data only, as determined by IRB or Data Use Agreement.

Data that could place the subject at severe risk of harm or data with contractual requirements for exceptional security measures

- Research data classified as Level 5 by the IRB
- Information or research under a contract stipulating specific security controls beyond L4



L5 – Reserved for project-specific data only, as determined by the project team or any industry requirements

Data that could place the subject at severe risk of harm or data with contractual requirements for exceptional security measures

Adopted from Harvard University -- https://policy.security.harvard.edu/

What have we discussed so far?

Information Security Handbook form NIST #SP 800-100 (2007)

Main Areas (content)

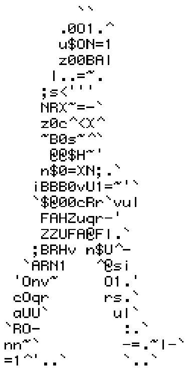
Important Control: Information Security Policy

A practical Example from Harvard University

And now ...

Coaching Task #3

I&CS – Coaching Session #3



And now?

Lets discuss coaching session #3

see seperate slide deck