THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

| UT Health Science Center:<br>GP-002-Data & System Classification | |
|---|---|
| **Version 7** | **Effective Date: 01/09/2022** |

| | |
|---|---|
| Responsible Office: Office of Cybersecurity | Last Review: 01/10/2022<br>Next Review: 01/10/2024 |
| Contact: Chris Madeksho | Phone: 901.448.1579<br>Email: mmadeksh@uthsc.edu |

# Purpose

At UTHSC, protecting our Institutional Information and IT Resources is critical to our mission of teaching, research, clinical care, and public service.

This Standard defines requirements for the appropriate classification of Institutional Information and IT Resources to ensure their confidentiality, integrity, and availability. It follows a risk-based approach to prescribe additional controls based on the need to achieve a specific level of protection for each category. UTHSC's investment in security controls is commensurate with the level of need for protection or availability of the Institutional Information

# Scope

This policy applies to any form of data, including paper documents and digital data stored on any type of media and the systems used to store, process, or transmit that data. It applies to all UTHSC employees, students, as well as to third-party agents authorized to access UTHSC data.

# Definitions

**Availability** – ensuring timely and reliable access to, and use of, information.
**Confidentiality** – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
**Information Technology (IT) Resources** – The collection of data and technology that support the achievement of organizational goals. IT Resources include hardware, software, vendors, users, facilities, data systems, and data.
**Integrity** – guarding against improper information modification or destruction and includes ensuring information accountability, non-repudiation, and authenticity.
**Security Categorization** - The process of determining the security category for data or an information system. Security categorization methodologies are described in Federal

Information Processing Standard (FIPS 199) and National Institute for Standards and Technology (NIST) SP 800-60. The security categorization helps identify the appropriate level of controls to be applied to the system or data.

## Responsibilities

**Data/System Owner** — The person who is ultimately responsible for the data and information being collected and maintained by their department or division, usually a member of senior management. The owner shall address the following:

- **Review and inventory** — Review and inventory IT resources within their areas of responsibility
- **Assignment of data and or system classification labels** — Assign classification based on the system or data type and potential impact level

**Data/System Custodian** – applying required security controls based on the classification, designated in GP-005-Data Security.

**Data Users** – the person who actually "touches" the information (enter, delete, read, process, etc.). Users are responsible for taking reasonable precautions against disclosure of data they have access to. Users should not grant access to data without proper authorizations from the Data Owner.

**Campus Units** – all units that collect and store data need to document their policies, procedures, and architectures that pertain to use, collection, and/or storage, regardless of the information format (electronic, paper, image, sound, etc.). This documentation should detail account creation and deletion, records retention and destruction, backup retention and destruction, and any other relevant procedures.

## Standard

1. Systems/Data need to be classified in each of the areas of Confidentiality (C), Integrity (I), and Availability (A).

2. The process of data and system classification is accomplished by assigning a classification score of 0-3 in the areas of Confidentiality, Integrity, and

Availability, with higher scores representing a higher level of sensitivity or criticality. It is acceptable if these are mixed, i.e. Confidentiality 1 (C-1), Integrity 3 (I-3), and Availability 2 (A-2). Each system/dataset will have different levels of security needs and controls based on risk and this classification process allows for the appropriate application of controls for each area. This process and examples are illustrated in Appendix A.

3. While selecting classification levels, System/Data Owners should also assign an impact level in the areas of Confidentiality, Integrity, and Availability to quantify the potential impact of an adverse event in each of these areas. This process, along with examples and definitions, is illustrated in Appendix A.

4. Data types should be identified and documented for each type of data that is transmitted, processed, or stored by the system or data set. These data types may have additional statutory requirements that must be assessed regarding security control implementation in addition to the baseline controls outlined in this standard. Data types that may need to be identified and associated with a system or data set are listed in Appendix B.

5. The classification of data is independent of its format. For example, if personal health information is revealed in a video recording of a lecture, then that video file should be classified as C-3. If paper credit card receipts are stored, then they should be classified as C-3.

6. Questions about classifying or handling the data should be directed to the Data Owner, your supervisor, the Office of Cybersecurity. The Office of Cybersecurity can assist departmental users in developing appropriate controls and processes to protect data based on the classification rating.

7. Report the misuse or compromise of systems that handle, store, or propagate any classification ranking one or above IMMEDIATELY to the Office of Cybersecurity at itsecurity@uthsc.edu.

Additional considerations:

- Data is scattered everywhere; data is stored, processed, and transmitted across numerous systems, devices, and users. The classification remains with the data and required protections follow that data.
- Context matters: the classification and impact ratings of the system/data depends on factors such as how it used or accessed, who is using it, the volume of data, etc., and not solely on the information alone.
- The Institutional Review Board (IRB) may have additional policies or requirements regarding data associated with IRB approved studies that must be followed based on their compliance procedures.

## Appendix A

### Classification, Impact, and System Security Plan Assignment

The process of data and system classification can be accomplished by assigning a classification score of 0-3 in the areas of Confidentiality, Integrity, and Availability:

**Confidentiality**

UTHSC data and IT Resources are classified into one of four levels based on the level of concern related to confidentiality. C-3 requires the most security controls, and C-0 requires none.

The relationship between the confidentiality classification and potential impact can be seen in Figure 1.

| Classification Rating | Classification Definition | System Security Plan Assignment | Possible Impact Score | Impact to Confidentiality<br>The unauthorized use or disclosure of information resources could be expected to have: |
|---|---|---|---|---|
| C-0 | Data which there is no expectation for privacy or confidentiality and is available for immediate public access.<br><br>Examples include, but are not limited to:<br>-Public-facing informational websites<br>-Public directory information<br>-Job postings<br>-Published research | None | 1. Negligible | Negligible adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse or unauthorized access to financial, medical, or personal information. |

| | | | | |
|---|---|---|---|---|
| | -Press releases<br>-Campus maps | | | |
| C-1 | Data that is potentially sensitive and is not intended to be shared with the public. Private data generally should not be disclosed outside of the University without the permission of the data owner. Data for which unauthorized use, access, disclosure, or acquisition could result in minor damage or small financial loss or cause minor impact on the privacy of an | Low | | |

| | | | | |
|---|---|---|---|---|
| | individual.<br><br>Examples include, but are not limited to:<br>-Routine business records<br>-Routine email not containing C-2 or C-3 information<br>-Calendar information not containing C-2 or C-3 information<br>-Meeting notes not containing C2 or C3 information<br>-Draft research papers<br>-Unpublished research using publicly available data<br><br>-De-identified data not containing C-2 or C-3 information | | 2. Minor | Minor (minor damage or financial loss or cause minor impact on the privacy of an individual) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse or unauthorized access to financial, medical, or personal information. |

| | | | | |
|---|---|---|---|---|
| C-2 | Data whose unauthorized disclosure could result in moderate fines, penalties, or civil actions. Institutional Information of which unauthorized use, access, disclosure, or acquisition, could result in moderate to severe damage to UTHSC, its students, patients, research subjects, employees, community and/or reputation; could have a moderate to severe impact on the privacy of a small to large group; could result in moderate to severe financial loss; or could require legal action. This classification level also includes lower risk items that, when combined, represent increased risk.<br><br>Examples include, but are not limited to:<br>-UTHSC personnel records<br>-IT security information<br>-Security camera recordings | Medium | 3. Moderate | Moderate (moderate damage or financial loss or cause moderate impact on the privacy of a small group) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse or unauthorized access to financial, medical, or personal information. |
| | | | 4. Severe | Severe (significant fines/financial loss, penalties or civil actions, damage to UTHSC, its faculty, employees, students, patients, study participants, community and/or reputation related to a breach or compromise; or could require legal action) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse or unauthorized access to financial, medical, or personal information. |

| | | | | |
|---|---|---|---|---|
| | -Export-controlled research<br>-Educational records not containing PII<br>-Any type of PII not classified as C-3<br>-Medical devices supporting diagnostics not containing C-3 information<br>-Industrial control systems affecting operations | | | |
| C-3 | Data whose unauthorized disclosure could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UTHSC students, patients, research subjects, | High | | |

| | | | | |
|---|---|---|---|---|
| | employees, guests/program participants, UTHSC reputation, or the overall operation of the Location or essential services. This classification level also includes lower risk items that, when combined, represent increased risk.<br><br>Examples include, but are not limited to:<br>-Credit card information<br>-Financial aid information<br>-Controlled unclassified information (CUI)<br>-Protected health information (patient records)<br><br>-Limited data sets that still contain some identifying information<br>-Social security numbers<br>-Sensitive identifiable human subject research data<br>-Authentication information<br>-Sensitive data governed by a | | 5. Catastrophic | Catastrophic (regulatory action, civil or criminal violations, or significant risk affecting life and safety) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse or unauthorized access to financial, medical, or personal information. |

| | | | | |
|---|---|---|---|---|
| | contract which may include a DUA, BAA or other contractual obligations<br>-Other PII in large data sets<br>-Medical devices support care<br>-Industrial control systems affecting life and safety | | | |

Figure 1

## Integrity

UTHSC data and IT Resources are classified into one of four levels based on the level of concern related to integrity. I-3 requires the most security controls, and I-0 requires none.

The relationship between the *integrity* classification and potential impact can be seen in Figure 2.

| Classification Rating | Classification Definition | System Security Plan Assignment | Possible Impact Score | Impact to Integrity<br>The unauthorized, unexpected, or accidental modification, destruction, or deletion of information resources could be expected to have: |
|---|---|---|---|---|
| I-0 | A system, software, vendor, or data for which there is no expectation of integrity or accountability as it relates to unauthorized, unexpected, or accidental modification, destruction, or deletion to those systems, software, vendor, or data. | None | 1. Negligible | Negligible adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse, modification, or deletion of their financial, medical, or personal information. |

| | | | | |
|---|---|---|---|---|
| I-1 | A system, software, vendor, or data for which there is a baseline expectation of integrity or accountability as it relates to unauthorized, unexpected, or accidental modification, destruction, or deletion to those systems, software, vendor, or data. A loss of integrity would be expected to result in minor adverse impact to stakeholders and basic controls should be in place to prevent, detect, and recover from adverse events. | Low | | |
| | | | 2. Minor | Minor (minor damage or financial loss or cause minor impact on the privacy of an individual) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse, modification or deletion of their financial, medical, or personal information. |
| I-2 | A system, software, vendor, or data for which there is a moderate expectation of integrity or accountability as it relates to unauthorized, unexpected, or accidental modification, destruction, or deletion to those systems, | Medium | 3. Moderate | Moderate (moderate damage or financial loss or cause moderate impact on the privacy of a small group) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse, modification or deletion of their financial, medical, or personal information. |

| | | | | |
|---|---|---|---|---|
| | software, vendor, or data. A loss of integrity would be expected to result in moderate to severe adverse impact to stakeholders and relative controls should be in place to prevent, detect, and recover from adverse events. | | 4. Severe | Severe (significant fines/financial loss, penalties or civil actions, damage to UTHSC, its faculty, employees, students, patients, study participants, community and/or reputation related to a breach or compromise; or could require legal action) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse, modification or deletion of their financial, medical, or personal information. |
| I-3 | A system, software, vendor, or data for which there is a mission critical expectation of integrity or accountability as it relates to unauthorized, unexpected, or accidental modification, destruction, or deletion to those systems, software, vendor, or data. A loss of integrity would be expected to result in severe to catastrophic adverse impact to stakeholders and the highest level of controls should be in place to prevent, detect, and recover from adverse events. Statutory, regulatory and | High | 5. Catastrophic | Catastrophic (regulatory action, civil or criminal violations, or significant risk affecting life and safety) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against misuse, modification or deletion of their financial, medical, or personal information. |

| | | | | |
|---|---|---|---|---|
| | contract obligations are major drivers for this risk level. | | | |

Figure 2

## Availability

UTHSC Institutional data and IT Resources are also classified into one of four availability levels based on the level of business impact their loss of availability or service would have on UTHSC. Compromises to A-3 data or resources would cause the highest level of impact; compromises to A-0 would cause none. A-4 requires the most security controls.

The relationship between the *availability* classification and potential impact can be seen in Figure 3.

| Classification Rating | Classification Definition | System Security Plan Assignment | Possible Impact Score | Impact to Availability<br>The disruption of access to or use of information resources could be expected to have: |
|---|---|---|---|---|
| A-0 | A system, software, vendor, or data for which there is no expectation of availability as it relates to the disruption of access to or use of those systems, software, vendor, or data. | None | 1. Negligible | Negligible adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against adverse events impacting the availability of the UTHSC systems, software, vendors, or data. |

| | | | | |
|---|---|---|---|---|
| A-1 | A system, software, vendor, or data for which there is a baseline expectation of availability as it relates to the disruption of access to or use of those systems, software, vendor, or data. A loss of availability would be expected to result in minor adverse impact to stakeholders and basic controls should be in place to prevent, detect, and recover from adverse events. | Low | | |
| | | | 2. Minor | Minor (minor damage or financial loss or cause minor impact on the privacy of an individual) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against adverse events impacting the availability of the UTHSC systems, software, vendors, or data. |
| A-2 | A system, software, vendor, or data for which there is a moderate expectation of availability as it relates to the disruption of access to or use of those systems, software, vendor, or data. A loss of availability would be expected to result in | Medium | 3. Moderate | Moderate (moderate damage or financial loss or cause moderate impact on the privacy of a small group) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against adverse events impacting the availability of the UTHSC systems, software, vendors, or data. |

| | | | | |
|---|---|---|---|---|
| | moderate to severe adverse impact to stakeholders and relative controls should be in place to prevent, detect, and recover from adverse events. | | 4. Severe | Severe (significant fines/financial loss, penalties or civil actions, damage to UTHSC, its faculty, employees, students, patients, study participants, community and/or reputation related to a breach or compromise; or could require legal action) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against adverse events impacting the availability of the UTHSC systems, software, vendors, or data. |
| A-3 | A system, software, vendor, or data for which there is a mission critical expectation of availability as it relates to the disruption of access to or use of those systems, software, vendor, or data. A loss of availability would be expected to result in severe to catastrophic adverse impact to stakeholders and the highest level of controls should be in place to prevent, detect, and recover from adverse events. Statutory, regulatory and contract obligations are major drivers for this risk level. | High | 5. Catastrophic | Catastrophic (regulatory action, civil or criminal violations, or significant risk affecting life and safety) adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect faculty, employee, student, patient, or study participant interests, data, privacy, and financial future against adverse events impacting the availability of the UTHSC systems, software, vendors, or data. |

Figure 3

## Appendix B

## Data that Must be labeled as "C-3"

**"Classified" information**
Data in any format that has been determined classified: (i) pursuant to Executive Order 12958 as amended by Executive Order 13526, or any predecessor Order, to be categorized national security information; or (ii) pursuant to the Atomic energy Act of 1954, as amended, to be restricted Data (RD).

**Authentication information**
Authentication information is data used to prove the identity of an individual, system, or service. Examples include:

- Passwords
- Shared secrets
- Cryptographic private keys
- Hash tables

**Protected Health Information (PHI)**
Protected Health Information is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity, and can be linked to a specific individual

**Electronic Health Information (ePHI)**

ePHI is defined as any protected health information (PHI) that is stored in or transmitted by electronic media. Electronic media includes computer hard drives as well as removable or transportable media, such as a magnetic tape or disk, optical disk, or digital memory card. Transmission is the movement or exchange of information in electronic form. Transmission media includes the internet, an extranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media.

**Payment Card Information (PCI)**
Payment card information is defined as a credit card number in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date

- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

**Personal Identifiable Information (PII)**

PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical and/or health insurance information

**Family Educational Rights and Privacy Act of 1974 (FERPA)**

FERPA defines education records as any record that directly relates to a student and is maintained by an educational agency or a party acting on behalf of the institution. Examples of education records include, but are not limited to:

- Transcripts
- Degree audit reports
- Schedules of classes
- Class rolls
- Academic history reports
- Grade rolls
- Financial records

**Financial Student Aid (FSA) Data**

FSA data is protected by the Graham-Leach-Bliley Act (GLBA) and other security outlined by the Federal Financial Institutions Examination Council (FFIEC).

**Controlled Unclassified Information (CUI)**

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. CUI is often associated with DoD related information or other federally sensitive information processed or stored in non-federal information systems.

**General Data Protection Regulation (GDPR) Data**

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in or are citizens of the European Union (EU).

## References

1. NIST 800-53, Security and Privacy Controls for Information Systems and Organizations
2. NIST Glossary of Terms
3. UTSA IT Policy IT0115 – Information and Computer System Classification
4. Standards for Security Categorization of Federal Information and Information Systems (FIPS 199).
5. GP-005-Data Security