

## 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
				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.  Examples include, but are not limited to: -Public-facing informational websites -Public directory information -Job postings -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.

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

	<ul style="list-style-type: none"> <li>-Press releases</li> <li>-Campus maps</li> </ul>			
C-1	<p>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</p>	Low		

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

	<p>individual.</p> <p>Examples include, but are not limited to:</p> <ul style="list-style-type: none"> <li>-Routine business records</li> <li>-Routine email not containing C-2 or C-3 information</li> <li>-Calendar information not containing C-2 or C-3 information</li> <li>-Meeting notes not containing C2 or C3 information</li> <li>-Draft research papers</li> <li>-Unpublished research using publicly available data</li> <li>-De-identified data not containing C-2 or C-3 information</li> </ul>		<p>2. Minor</p>	<p>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.</p>
--	--	--	-----------------	--

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

C-2	<p>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.</p> <p>Examples include, but are not limited to:</p> <ul style="list-style-type: none"> <li>-UTHSC personnel records</li> <li>-IT security information</li> <li>-Security camera recordings</li> </ul>	Medium	3. Moderate	<p>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.</p>
			4. Severe	<p>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.</p>

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

	<ul style="list-style-type: none"> <li>-Export-controlled research</li> <li>-Educational records not containing PII</li> <li>-Any type of PII not classified as C-3</li> <li>-Medical devices supporting diagnostics not containing C-3 information</li> <li>-Industrial control systems affecting operations</li> </ul>			
C-3	<p>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,</p>	High		

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

	<p>employees, guests/program participants, UTHSC reputation, or the overall operation of the Location or essential services.</p> <p>This classification level also includes lower risk items that, when combined, represent increased risk.</p> <p>Examples include, but are not limited to:</p> <ul style="list-style-type: none"> <li>-Credit card information</li> <li>-Financial aid information</li> <li>-Controlled unclassified information (CUI)</li> <li>-Protected health information (patient records)</li> <li>-Limited data sets that still contain some identifying information</li> <li>-Social security numbers</li> <li>-Sensitive identifiable human subject research data</li> <li>-Authentication information</li> <li>-Sensitive data governed by a</li> </ul>		<p>5. Catastrophic</p>	<p>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.</p>
--	---	--	------------------------	---

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

	<p>contract which may include a DUA, BAA or other contractual obligations</p> <ul style="list-style-type: none"> <li>-Other PII in large data sets</li> <li>-Medical devices support care</li> <li>-Industrial control systems affecting life and safety</li> </ul>			
--	---	--	--	--

Figure 1

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

### Integrity

UTHSC data and IT Resources are classified into one of four levels based on the level of concern related to integrity. L3 requires the most security controls, and L0 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
				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.



<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

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.

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

	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.			
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	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.
			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.

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

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

Figure 2

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

### 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
				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.

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

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.

<b>UT Health Science Center: GP-002-Data &amp; System Classification</b>	
<b>Version 7</b>	<b>Effective Date: 01/09/2022</b>

	<p>moderate to severe adverse impact to stakeholders and relative controls should be in place to prevent, detect, and recover from adverse events.</p>			
A-3	<p>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.</p>	High	4. Severe	<p>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.</p>
			5. Catastrophic	<p>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.</p>