# TABLE OF CONTENTS

1.1 Scope 2
1.2 Principles 2
1.3 Revisions 3
2.1 Objective 4

3.1 Program Details 4
3.2 Media Storage and Access 4
3.3 Media Transport 4
3.4 Media Sanitization 4
3.5 Removable Media 5

4.1 Mandatory Controls 5

5.1 Discretionary Controls 6

6.1 References 6

7.1 Definitions 6
1.1 SCOPE
This program applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee at Martin (UTM) including its remote centers.

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the university’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

1.2 PRINCIPLES
UTM has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications, and this program is based on those guidelines. Specifically, this program is based on the Media Protection Control Family principles found in NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

UTM must develop or adopt and adhere to a program that demonstrates compliance with related policies and standards. This program is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance University policy is assumed if a User accesses, uses, or handles University IT resources.
## 1.3 REVISIONS

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/10/2014</td>
<td>Created (0.1)</td>
<td>Will Turner</td>
</tr>
<tr>
<td>11/14/2014</td>
<td>Revised (0.2)</td>
<td></td>
</tr>
<tr>
<td>11/20/2014</td>
<td>Reformatted University template (0.3)</td>
<td></td>
</tr>
<tr>
<td>01/16/2015</td>
<td>Reformatted to new University template (0.4)</td>
<td></td>
</tr>
<tr>
<td>01/20/2015</td>
<td>Made corrections per Amy (0.5)</td>
<td></td>
</tr>
<tr>
<td>03/10/2015</td>
<td>Changed wording (0.6)</td>
<td></td>
</tr>
<tr>
<td>06/22/2016</td>
<td>Reformatted to newer UTSA template; wording (0.7)</td>
<td>Brian Stubblefield</td>
</tr>
<tr>
<td>07/27/2016</td>
<td>Changed title, added reference to sanitization policy (0.8)</td>
<td></td>
</tr>
<tr>
<td>11/28/2016</td>
<td>Recommendations by Mark, new template, layout, contents (0.9)</td>
<td></td>
</tr>
<tr>
<td>02/03/2017</td>
<td>Finalize contents for review (0.10)</td>
<td></td>
</tr>
<tr>
<td>08/22/2017</td>
<td>Multiple changes to content and/or formatting (0.11)</td>
<td></td>
</tr>
<tr>
<td>08/23/2017</td>
<td>Recommended changes, CoP updates (0.12)</td>
<td></td>
</tr>
<tr>
<td>09/18/2017</td>
<td>Updates to controls, wording, and document versioning (0.13)</td>
<td></td>
</tr>
<tr>
<td>10/25/2017</td>
<td>Suggested changes from Amy (0.14)</td>
<td></td>
</tr>
<tr>
<td>11/07/2017</td>
<td>Changed definition for PII (0.15)</td>
<td></td>
</tr>
<tr>
<td>11/27/2017</td>
<td>Approved (1.0)</td>
<td></td>
</tr>
</tbody>
</table>
2.1 OBJECTIVE
The purpose of this program is to manage risks from media access, media storage, media transport, and media protection through the establishment of an effective Media Protection Program (MP-1). This program allows UTM to comply with University requirements as well as ensures the effective management of all media containing sensitive information (from inception through disposal).

3.1 PROGRAM DETAILS
This program provides reasonable assurance, in proportion to the sensitivity of the data, that media containing Sensitive Information is protected from unauthorized access, and is sanitized or destroyed before disposal, reuse, or release out of organizational control.

All policy-related standards and procedures must be consistent with applicable laws, regulations, and guidance. This program and all associated standards and procedures as well as their implementation effectiveness must be reviewed annually and updated as needed (MP-1).

3.2 MEDIA STORAGE AND ACCESS
All departments must physically control and securely store Sensitive Media within secure areas using physical security controls and safeguards until the media is destroyed or sanitized (MP-4). Sensitive Media should never be left unattended (ex. on a desk or printer, in a lab, etc.).

Access to Sensitive Media must be restricted to authorized personnel (MP-2).

3.3 MEDIA TRANSPORT
Strong encryption is required to protect the confidentiality and integrity of Sensitive Media during transport outside of controlled areas. Activities associated with the transport of such media must be restricted to authorized personnel (MP-5).

3.4 MEDIA SANITIZATION
All UTM departments and affiliates must sanitize Sensitive Media, both digital and non-digital, prior to disposal, reuse, or release from organizational control using approved recommendations and methods (MP-6).

Recommendations and methods are established in the Media Sanitization Standard.
3.5 REMOVABLE MEDIA
The use of removable/portable media devices may be restricted on campus, when necessary. Methods of restriction include but are not limited to disabling or physically blocking ports, approved devices, and device types (MP-7).

Unknown Removable Media should never be connected to or inserted into any system. It should be treated as malicious until verified.

Personally Identifiable Information (PII) should never be stored on removable media. If PII is required to be stored on removable media for official University business, strong encryption must be used and validated.

4.1 MANDATORY CONTROLS
Mandatory security controls are university-wide controls that are required to be consistently designed, implemented, monitored, and assessed.

- **Policy and Procedures (MP-1):** Each Campus must develop or adopt and maintain a media protection program that includes the implementation of this policy and associated controls, and an annual review of that program.
- **Media Access Restrictions (MP-2):** Each Campus must restrict access to Sensitive Media, both digital and non-digital, that contains Sensitive Information (information classified as Moderate or High per University Policy IT0115, Classification).
- **Media Storage (MP-4):** Each Campus must store all Sensitive Media within secured, access-controlled areas and secure that media until destroyed or sanitized using approved equipment, techniques, and procedures.
- **Media Transport (MP-5):** Each Campus must protect Sensitive Media during transport outside of controlled areas and restrict the activities of such media to authorized personnel.
- **Media Sanitization (MP-6):** All Campuses must sanitize Sensitive Media, both digital and non-digital, prior to disposal, reuse, or release out of organizational control.
- **Media Use (MP-7):** UTM may restrict the use of portable storage devices:
  - by using physical means to prohibit access to certain external ports or disabling/removing the ability to insert, read or write to such devices;
  - to only approved devices, including but not limited to those provided by the University or other approved organizations and that are not personally owned;
  - based on the type of device by disabling or removing the capability to write to such devices.
5.1 DISCRETIONARY CONTROLS
Discretionary Controls are security controls whose scope is limited to a specific campus, institution, or other designated organizational component. Discretionary Controls are designed, implemented, monitored, and assessed within that organizational component. Discretionary controls must not conflict with or lower the standards established by Mandatory Controls.

6.1 REFERENCES
NIST SP 800-53 Revision 4 - Recommended Security Controls for Federal Information Systems and Organizations

NIST SP 800-88 Revision 1 - Guidelines for Media Sanitization

Media Sanitization Standard

7.1 DEFINITIONS
Access-controlled areas - Areas in which organizations provide sufficient physical and procedural safeguards necessary to protect information and/or information systems.

Digital media - Includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

Encryption - The process of converting information or data into a special form to prevent unauthorized access.

Medium (pl. Media) - Material, both digital and non-digital, on which information may be stored.

Non-digital media - Includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers.
**Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

**Removable Media** - Any type of storage device that can be inserted and removed from a computer while the system is running; This includes but is not limited to USB flash drives, external hard drives, optical discs (CD, DVD, Blu-ray), memory cards (Secure Digital (SD), microSD, Memory Stick, compact flash), floppy or zip disks, and other storage devices (digital camera, mobile phone, multimedia player).

**Sanitization** - A process to render access to Target Data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media.

**Secure storage** - Includes, for example, a locked drawer, desk, or cabinet, or a controlled media library.

**Sensitive Information** - Information that is protected against unwarranted disclosure. Protection of sensitive information may be required for legal, ethical, privacy, or proprietary considerations. Sensitive information includes all data which contains: Personally Identifiable Information, Protected Health Information, student education records, card holder data, or other information that is protected by applicable laws, regulation, or policies.

**Sensitive Media** - Digital or non-digital media that contains Sensitive Information.

**Strong Encryption** - An encryption method utilizing a very large number (greater than or equal to 256 bits) as its cryptographic key.

**Unknown Removable Media** - Removable media of unknown origin and contents