Standard Practice for Assessment of Impact of Mobile Data Storage Device (MDSD) Loss[1]

This standard is issued under the fixed designation E 2674; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This practice describes a methodology for assessing and quantifying the impact of the loss of mobile data storage devices (MDSDs), for example, thumb drives, auxiliary hard drives, and other property containing personally identifiable information or other entity sensitive information.

1.2 This practice is based on two concepts:

1.2.1 Identifying the MDSDs that pose the greatest risk to the organization based on both the information that is stored on them and the location in which they are used, and

1.2.2 Determining the impact of the potential loss of specific MDSDs. In general, this impact assessment is best practiced as a part of a larger risk management process. While this practice does not address this larger topic, it may inform other risk management standards.

1.3 This practice is intended to be applicable and appropriate for all asset-holding entities.

1.4 In accordance with the provisions of Practice E 2279, this practice clarifies and enables effective and efficient control and tracking of equipment.

1.5 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 *ASTM Standards:*[2]

E 2135 Terminology for Property and Asset Management

E 2279 Practice for Establishing the Guiding Principles of Property Management

E 2452 Practice for Equipment Management Process Maturity (EMPM) Model

E 2495 Practice for Prioritizing Asset Resources in Acquisition, Utilization, and Disposition

E 2499 Practice for Classification of Equipment Physical Location Information

E 2608 Practice for Equipment Control Matrix (ECM)

3. Terminology

3.1 *Definitions*—For definitions relating to property and asset management, refer to Terminology E 2135.

3.1.1 *compliance impact*, *n*—consequence of loss of control characterized by negative compliance with applicable laws, regulations, or other relevant internal or external guidance that does not rise to the level of an operational impact. **(E 2608)**

3.1.2 *consequence*, *n*—the effect of actions (something that logically or naturally follows from an action or condition).

3.1.3 *equipment control classes (ECCs)*, *n*—classifications or groupings of equipment based on the consequences of the loss of control of the equipment. **(E 2608)**

3.1.4 *operational impact*, *n*—consequence of loss of control characterized by negative operational impact that does not rise to the level of a personal or societal safety or security impact. **(E 2608)**

3.1.5 *organizational impact*, *n*—objects that affect or influence the capability of an entity, especially in a significant or undesirable manner.

3.1.6 *personal safety/security consequence*, *n*—consequence of loss of control characterized by negative personal safety or security impact that does not rise to the level of a societal safety or security impact. **(E 2608)**

3.1.7 *probability*, *n*—or chance that something is the case or will happen.

3.1.8 *risk*, *n*—concept that denotes a potential negative impact.

3.1.9 *risk assessment*, *n*—determination of the quantitative or qualitative value of risk related to a concrete situation and a recognized threat.

3.1.9.1 *Discussion*—It is considered as the initial and a recurring step in a risk management process.

[1] This practice is under the jurisdiction of ASTM Committee E53 on Property Management Systems and is the direct responsibility of Subcommittee E53.02 on Data Management.

Current edition approved Feb. 1, 2009. Published February 2009.

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

3.1.10 *risk management*, *n*—structured approach to managing uncertainty through risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources.

3.1.10.1 *Discussion*—The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

3.1.11 *societal safety/security consequence*, *n*—consequence of loss of control characterized by negative societal safety or security impact. **(E 2608)**

3.2 *Definitions of Terms Specific to This Standard:*

3.2.1 *information system*, *n*—any computerized data processing system.

3.2.2 *information type*, *n*—category of data at any stage of processing (input, output, storage, transmission, and so forth).

3.2.3 *personally identifiable information (PII)*, *n*—any information about an individual maintained by an entity, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual.

3.2.4 *mobile data storage device (MDSD)*, *n*—any tangible asset capable of storing human or machine-readable data.

3.3 *Acronyms:*

3.3.1 *ECC*—equipment control class

3.3.2 *ECL*—equipment control level

3.3.3 *PII*—personally identifiable information

3.3.4 *PLL*—physical location level

3.3.5 *MDSD*—mobile data storage device

3.3.6 *NISPOM*—National Industrial Security Program Operating Manual

4. Significance and Use

4.1 This practice establishes a standard impact assessment methodology to enable entities to uniformly ascertain and communicate impact levels associated with the potential loss of MDSDs. This practice is not intended to prescribe specific information security policies for entities or organizations. This practice assumes that individuals and entities are following all relevant information security policies as required by federal or state law, the terms of applicable government contracts, specific agency policies such as the National Industrial Security Program Operating Manual (NISPOM), and entity-specific policies.

4.2 This practice assumes, but does not require, that entities have devised and are maintaining a system of internal controls over MDSDs in accordance with the section on Management of Property of Practice E 2279.

4.3 This practice assumes, but does not require, that the results of this impact assessment will inform future actions and help entities determine cost-effective property control measures for MDSDs commensurate with the potential consequences of their loss in accordance with the section on Management of Property of Practice E 2279.

4.4 This practice encourages an inclusive understanding and communication of the risk associated with MDSDs and, by assigning a rating to the impact of loss, enables comparisons on this basis to other MDSDs rated using the same practice.

4.5 This practice is intended to foster and enable additional standard practices related to or based on these terms and concepts.

5. Impact Assessment

5.1 The intended outcome of this practice is to create a quantitative index of the MDSDs that pose the consequence of loss based on:

5.1.1 The information systems or information types, or both, to which individuals have access and thus are likely to be stored on a device under that individual's control,

5.1.2 The MDSDs under an individual's control, and

5.1.3 The location in which the MDSD is normally used.

5.2 *Consequence*—Practice E 2608 details equipment control classes (ECCs) designed to provide standard classes for equipment based on control and tracking requirements for the equipment. This approach and nomenclature are adapted for use in this practice as consequence levels to represent the consequences of loss of control of MDSDs.

5.2.1 *Consequence Level 1*—Consequence of loss of control is a societal safety/security impact that is characterized by negative societal safety or security impact.

5.2.2 *Consequence Level 2*—Consequence of loss of control is a personal safety/security impact that is characterized by negative personal safety or security impact that does not rise to the level of a societal safety or security impact.

5.2.3 *Consequence Level 3*—Consequence of loss of control is an operational impact that is characterized by negative operational impact that does not rise to the level of a personal or societal safety or security impact.

5.2.4 *Consequence Level 4*—Consequence of loss of control is a compliance impact that is characterized by negative compliance with applicable laws, regulations, or other relevant internal or external guidance that does not rise to the level of an operational impact.

5.2.5 *Consequence Level 5*—Consequence of loss of control is not discernible, that is, characterized by having no visible or recognizable impact on the organization.

5.3 *Location of Use*—This practice outlines three broad locations where MDSDs may be used. The nature of the location where a device is used largely determines the level of physical control to which a device is normally subject and thus influences the probability of loss. The following locations of use may be added to or further subdivided by an assessing entity to accommodate the particular levels of security or physical control established for different areas at or within a particular physical location level (PLL) as described in Practice E 2499.

5.3.1 *Mobile*—MDSDs frequently move between sites (PLL 5), and thus present the greatest probability of loss. MDSDs may be used in a combination of secured and unsecured sites. Examples include flash drives, personal digital assistants (PDAs), mobile telephones, and laptops.

5.3.2 *Offsite*—MDSDs used in offsite locations are not subject to the direct physical custody of the owning entity but do not normally move from one building (PLL 6) to another. As such, these devices present a moderate probability of loss.