EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

Policy

Effective Date	Date of Last Revision
April 26, 2010	

Chapter Name	
8.0 Security	
Chapter Number	**Title**
8.5	**Security Controlled Spaces**

1.0 Purpose

To safeguard the integrity of Eastern Michigan University's (EMU) information resources, it is mandatory that physical access to the security controlled spaces be restricted and all access be logged and monitored. The purpose of this policy is to prevent accidental or intentional damage, theft, sabotage or loss of data or equipment used to maintain University information systems.

2.0 Scope

This policy applies to any and all Division of Information Technology (DoIT) managed EMU data center(s), computer rooms and communications closets (collectively referred to as "security controlled spaces"). This policy covers any and all persons (employees, vendors, visitors and others) needing access to security controlled spaces for legitimate reasons. There are University locations in which DoIT maintains equipment, and these spaces are accessed by both DoIT personnel and personnel from other EMU divisions. These spaces are called Dual Access Security Controlled Spaces and are not covered by this policy.

3.0 Policy

It is the policy of DoIT to secure and limit physical access to all security controlled spaces managed by DoIT.

DoIT may use video cameras, covert video cameras and video recording devices for surveillance and monitoring purposes of access to security controlled spaces.

DoIT may use alarm systems to detect and alert University police and DoIT administration of physical intrusion/unauthorized access into security controlled spaces.

This policy does not preclude DoIT from using security tools, techniques or systems not explicitly defined in this policy. Specific tools listed here are examples of the types of tools that may be used, not an explicit list of those tools that are permitted.

DoIT employees' physical access shall be limited to the minimal access necessary to complete job duties. Primary security controlled access shall be granted to approved employees via ID card reader. A secondary method for controlled access is by an assigned key and will only be used for entrance into non-card reader protected locations or when ID card reader is inoperable.

All access by individuals not authorized to enter security controlled spaces via the ID card system must obtain permission from an authorized IT staff to enter the space. and shall be logged. The log shall be reviewed periodically.

Authorized IT staff must personally escort unauthorized persons into security controlled spaces.

DoIT staff members are only permitted to enter security controlled spaces to which they have been explicitly authorized. Staff members who enter security controlled spaces without authorization/escort or staff members who provide access to unauthorized persons are subject to appropriate disciplinary action.

4.0 Responsibility for Implementation

The Director of Network and Systems Services or his/her designees are responsible for implementing this policy. Working within the terms of this policy, the director or designees shall cause the configuration, maintenance and monitoring card readers, keypads and other security devices to ensure that only authorized staff members have access to appropriate spaces.

5.0 Enforcement

The Associate Director, Enterprise Operations Center, and the Director of Network and Systems Services as well as the rest of the DoIT Leadership staff are responsible for the enforcement of this policy and for initiating progressive disciplinary action or termination for violations of this policy.

6.0 Definitions

Term	Definition
Dual Access Security Controlled Spaces	Spaces where DoIT maintains equipment and which spaces can be accessed by DoIT personnel and personnel from other EMU divisions.
Security controlled spaces	Computer rooms, data centers and communications closets housing DoIT managed equipment, servers or other hardware/software systems.

7.0 Revision History

Description	Approval Date
Original	April 23, 2010