The University of North Texas at Dallas Policy Manual	Chapter 14.000
14.009 Physical Access	**Information Technology**

Policy Statement. It is the policy of the University of North Texas at Dallas to manage the University's information resources as strategic assets of the State of Texas. The Physical Access Policy establishes the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

Application of Policy. This policy applies to the total university.

Definitions.

1. Information Resources (IR). "Information Resources" mean any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

2. Information Services (IS). "Information Services" mean the name of the agency department responsible for computers, networking and data management.

Procedures and Responsibilities.

1. **General Provisions**.

   1.01. All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.

   1.02. Physical access to all restricted facilities housing, storing, or containing Information Resources must be documented and managed.

   1.03. All Information Resources facilities must be physically protected in proportion to the criticality or importance of their function.

   1.04. Access to Information Resources facilities must be granted only to support personnel and contractors, whose job responsibilities require access to that facility. Access to facility will be granted for only the time period in which their responsibilities require access.

   1.05. The process for granting card and/or key access to Information Resources facilities must

include the approval of the person responsible for the security of the facility.

1.06. Each individual that is granted access rights to an Information Resources facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.

1.07. Requests for access must come from the applicable data/system owner.

1.08. All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.

1.09. Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.

1.10. The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals that change roles within the University or are separated from their relationship with the University.

Responsible Party: Information Resource Owner/Information Technology

2. **Access Provisions**.

2.01. Access cards and/or keys must not be shared or loaned to others.

2.02. Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process.

2.03. Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility.

2.04. A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.

Responsible Party: All University Users/ Information Technology

References and Cross-references.

Texas Government Code § 2054 - Information Resources

Texas Administrative Code § 202.73

Approved: 8/30/2010
Effective: 8/30/2010
Revised: