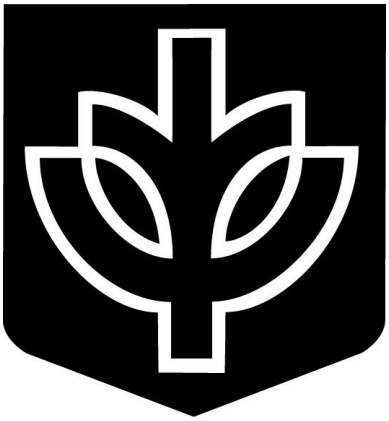
DATA CENTER ACCESS POLICY AND GUIDELINES



Information Security Team
DePaul University
1 East Jackson Boulevard
Chicago, Illinois 60604
https://infosec.depaul.edu/

13th December 2002

Copyright Notice

Contents

1 Summary

This policy is a recommendation for dealing with access to secured physical areas housing computers, network devices and other critical infrastructure computing components that support current services. Too often physical security is overlooked at by operational staff as an afterthought; physical security and compliance with guidelines can be costly and yield low benefits to all but the site's operational staff. Likewise, procedures can be difficult to following and maintain as new technologies are deployed at the site.

The implementation of any policy or guideline requires a methodical set of procedures to be developed for assisting all those affected. A sample of these guidelines can be found in this document as a recommendation for your site when developing guidelines. Additionally, this document may be used directly as a guideline to meet your basic requirements.

2 Access Authorization Requests

A central point of contact should be assigned for each data center, network closet or operations facility. These contacts should be delegated by the responsible director or manager claiming responsibility for the physical area, and maintenance thereof.

2.1 Requesting Access

An individual requiring physical access to a restricted area should obtain the necessary forms for access to the physical location — these forms may be specific to an area depending on the requirements, etc. A completed form should be sent to the appropriate contact(s) for the area; we *strongly recommend* a digital signature be used to authorize requests. Where critical infrastructure components are held, only an email signed by a valid digital key should be acknowledged. Further, INFOSEC strongly recommends that each responsible area promote the use of digital encryption when submitting request information.

2.2 Reservation of Access Rights

Each responsible entity for a data center should include a disclaimer that access to secured area may be revoked temporarily or permanently for any reason, at any time. These guidelines should included in the necessary access forms to the area and agreed to each person requesting access to the secured areas.

2.3 Emergency Access

Emergency access to a secured site should not be permitted. Each resource should have primary and secondary *authorized* personnel "on call" ready to respond to a situation at all times. Proper cross-training and contact information should be developed to promote limiting of emergency access completely.

3 Guidelines for Use

Each access to the data center should be made in compliance with the following guidelines in order to increase the longevity of systems. While other specific guidelines may be required for a specific site requirement, these general guidelines should retrofit existing installations.

1. Access to all secured areas should require the use of an authorized swipe card, proxy card, biometric device, physical key or password. Where possible, all entries into the secured areas should be recorded and reviewed by the responsible parties for the area. *All* access should be logged, even when a group of persons enters the area.

2. Swipe cards and proxy cards should not be shared between authorized and unauthorized persons.

3. A seperate log should be kept for "sign-in" to the area. This log book should record a name, employee identification number, time in, time out, and signature.

4. Vendors, or those wishing to access the data center for a specific task, should be accompanied by an authorized person at *all* times.

5. The secured area should only be accessed to meet a business requirement. When such a requirement is complete, leave the area. Do not loiter.

6. A resource in use (computer, monitor, keyboard, network cable, power cable, cabinet, floorboard, etc.) should be moved only by the person directly responsible for that resource.

7. Food, drink or other fluids must not be introduced to the secured areas. These items promote deterioration of computing hardware through moisture.

3.1 Physical Security Measures

The physical security measures implemented at each secured site will greatly assist in the compliance with policy. Monitoring devices and access control devices should record each entry into the secured area, both authorized and unauthorized. A log of entries should be archived for a period of two (2) years. If the site is monitored with video or audio devices, this data should too be archived.

A Sample Access Request Form

The following form may be used as a template when building an access control policy or guideline for a secured area.

```
  Data Center Access Request Form for [Sample Data Center]

Copyright Notice
----------------

  Copyright (C) 2002. DePaul University. All Rights Reserved.

Access Policies
---------------

Access request to [Sample Data Center] may be obtained by
submitting this form to <dcrequest@example.org>. This form should
be digitally signed and encrypted where possible.

By requesting this access you explicitly agree to all policies and
guidelines set forth by [Sample Data Center] management staff, and
validate that the employee requiring access has been made aware of
all policies and guidelines that pertain to [Same Data Center]. You
may also be held liable for any action or damages against [Sample
Data Center]. [Sample Data Center] management staff reserves the
right to revoke access to the area(s) at any time, for any reason,
without prior notification.

Section I - Employee Information
--------------------------------

 Employee Requiring Access
   - Name: _____________________________________________________
   - Title: ____________________________________________________
   - Phone: ____________________________________________________
   - Email: ____________________________________________________
   - Division: _________________________________________________
   - Department: _______________________________________________
   - PGP Key ID: _______________________________________________
   - Fingerprint _______________________________________________
   - Employee ID: ______________________________________________
   - SSN: ______________________________________________________
```

Section II - Approving Manager or Director

Approving Manager or Director (if different)
- Name: _____
- Title: _____
- Phone: _____
- Email: _____
- Division: _____
- Department: _____
- PGP Key ID: _____
- Fingerprint _____

Section III - Type of Access

This access is to begin on __/__/____ at __:__ CST.

This employee should be allowed to access the area -
[ ] during normal business hours (M-F 08:00 - 18:00).
[ ] at all times.
[ ] from __:__ CST to __:__ CST [ ] Weekdays
__:__ CST to __:__ CST [ ] Weekends
__:__ CST to __:__ CST [ ] Holidays

Access should be allowed -
[ ] Permanently.
[ ] Temporarily, ending on __/__/____ at __:__ CST.

Please state the requirements to be filled by such access.
_____
_____
_____

$Id: dcaccessform.tex,v 1.4 2002/12/10 21:54:46 eric Exp $