Data Centers and Mission Critical Facilities
Access and Physical Security Procedures

Attachment B
(Referenced in UW Information Technology Data Centers and Mission Critical Facilities Access and Physical Security Policy)

Updated: 11/14/2010
Created: 05/14/2010
Planning & Facilities
Data Centers & Facilities Management
206.221.4500
uwtech-facilities@uw.edu
1.0  Purpose

1.0.1  In support of the University of Washington Information Technology Data Centers and Mission Critical Facilities Access and Physical Security Policy, these procedures provide a strong security strategy that protects UW Information Technology (UW-IT) employees and the data and resources entrusted to UW-IT by the University of Washington and by UW-IT customers. UW-IT building and location security is a fundamental component of the overall UW-IT security plan. These procedures are intended to clarify access requirements for all UW-IT centrally managed data centers and mission critical facilities including the University campus and off-campus leased data centers and mission critical facilities.

2.0  Issuing Office

2.0.1  The UW-IT unit of Planning & Facilities, Data Center & Facilities Management (DCFM), is responsible for issuing all security badges, authorization forms and hard keys through its DCFM Access Control office. DCFM Access Control is the security liaison between the University of Washington (UW), UW-IT and its co-location customers for access into all UW-IT centrally managed data centers, owned or leased. DCFM Access Control is responsible for the management of all active and inactive records of authorized security badges. All records are maintained according to the UW Records Management retention schedule assigned by the University to the DCFM Access Control office.

3.0  Communication of Policy

3.0.1  All UW-IT managers, supervisors, sponsors of co-location tenants, and authorizing co-location unit heads (or their designees) will communicate to, and review with, new and current employees the stipulations within this policy and its procedures, and are responsible for ensuring that all employees are compliant with this policy. All changes in employee duties will require a review of data center access requirements.

3.0.2  All authorized UW-IT staff members and co-location tenants who escort authorized contractors or co-workers into a UW data center must communicate this policy to the escorted contractor and ensure their compliance at all times.
3.0.3 All authorized UW-IT contractors and co-location tenant contractors who have approved, unescorted access into a UW-IT centrally managed data center must read and understand this policy and ensure that they, and all workers associated with them, are compliant with this policy at all times.

4.0 Security Badge Sponsors

4.0.1 Responsibilities of the badge sponsor include, but are not limited to, authorizing badge requests, reviewing badge access, and requesting badge expiration extensions.

4.0.2 For UW-IT employees and UW co-location tenants, the unit head (or unit head’s designee) will act as the badge sponsor.

4.0.3 For contractors performing services for UW-IT or co-location tenants, the unit head (or unit head’s designee) of the contracting UW department or co-location organization will act as the badge sponsor.

4.1 Types of Security Badges

4.1.1 DCFM Access Control is responsible for activating, making any access modifications to, and terminating all security badges. There are five types of security badges: permanent employee; permanent contractor; temporary; escort-only; and visitor.

4.1.2 Permanent Employee Badges: Employee security badges are issued to UW-IT permanent, hourly, temporary, and student employees and to co-location customers with long-term agreements with UW-IT. Permanent employee security badges display pictures of the badge holder for identification.

4.1.3 Permanent Contractor Badges: Contractor badges are issued to contractors who perform data center system maintenance or service (with an agreement for longer than six months) and who respond to UW data centers for emergencies. These badges may or may not display pictures of the badge holder. Contractor badges are activated for a defined period of time, not to exceed six months from the date of issue. Requests for extension will be reviewed on a case-by-case basis. Contractor badges should remain on-site at the UW data center for the contractors to sign out as needed. With prior approval from the unit head (or unit head’s designee), a badge may be kept in the contractor’s possession for the duration of their contract.
4.1.4 Temporary Badges: Temporary security badges are issued as replacements for lost or damaged permanent badges, and are only issued to pre-existing, approved, permanent badge holders. When a temporary security badge is issued, all policies and procedures remain in effect. Temporary badges are activated for a 24-hour period. Temporary badges must be returned to DCFM Access Control at or before the end of the activation period. Requests for extensions will be reviewed on a case-by-case basis.

4.1.5 Escort-Only (E) Badges: Escort-only badges are assigned to UW employees, co-location employees and contractors who do not have permanent or temporary security badges, but must perform maintenance or service in a UW-IT centrally managed data center. Escort-only badges do not grant badge reader access to any data center, and the badge holder must be accompanied by a pre-approved escort at all times. When an escort-only badge is issued, all policies and procedures remain in effect. Only authorized UW personnel and authorized UW co-location customers who possess authorized access may escort other staff, contractors or vendors into a data center. Escort-only badges must be returned to DCFM Access Control before the badge holder leaves the premises.

4.1.6 Visitor (V) Badges: Visitor badges are issued to all guests who have been pre-approved for data center tours or site visits. Visitor badges do not grant badge reader access to any data center, and the badge holder must be accompanied by a pre-approved escort at all times. Only authorized UW personnel and authorized UW co-location customers who possess authorized access may escort visitors into a data center. When a visitor badge is issued, all policies and procedures remain in effect. Visitor badges must be returned to DCFM Access Control before the badge holder leaves the premises.

4.2 UW-IT–Issued Security Badge Appearance, Both Leased and Owned

4.2.1 In order to provide distinction between the different types of badges authorized to access UW data centers, a color code has been determined.

4.2.2 All other badges issued from leased locations will have their own unique color and identifying markings that indicate authorized data center access.

4.3 Obtaining New Permanent Security Badges

4.3.1 In order to be granted data center access, the applicant’s badge sponsor must complete the required UW-IT DCFM Access Control form. Additional forms may be required when requesting access to UW-IT leased data center spaces. These additional forms are available from DCFM Access Control upon
request. DCFM Access Control will process each security badge request, and upon approval will contact the applicant to arrange an appointment for a badge photo (if required) and issuance of the badge.

4.3.2 Applicants must present government-issued photo identification to DCFM Access Control and allow for the verification of the name and identity of the badge holder. For applicants of permanent badges, including UW employees, co-location employees and contractors, a successful background check is a prerequisite for data center access.

4.3.3 For contractors performing services for UW-IT or co-location tenants, all applications for data center access must be accompanied by an original (not a copy) letter stating that a background check has been successfully performed with positive results on the applicant. The letter must be prepared by the contracting company’s management or human resources department on company letterhead and dated within 90 days preceding the request for data center access. A sample for background checks may be found at this Web site: Washington State Patrol WATCH program: http://www.wsp.wa.gov/crime/crimhist.htm.

4.3.4 Any request for exception to this procedure must be in writing from the badge sponsor, and will be reviewed on a case-by-case basis. An allowable exception could include a UW employee whose pre-employment requirements did not include any form of background check.

4.4 Obtaining Replacement Permanent Security Badges

4.4.1 Damaged Badge: Requests for replacement of a damaged badge will be processed within two working days of receipt of the request by DCFM Access Control, unless a new badge photo is required. The badge holder must turn in the damaged badge to DCFM Access Control before a replacement badge will be issued. If required, a temporary badge will be issued until the replacement badge is ready.

4.4.2 Lost Badge: Requests for replacement of a lost badge will be processed after a two-week waiting period from the time of request to DCFM Access Control. The waiting period allows for the possible return of the original badge. The requesting employee must submit an incident report for the lost badge to DCFM Access Control before a replacement badge will be issued. If required, a temporary badge will be issued until the replacement badge is ready.
4.4.3 New Photo: A new photo is mandatory for any damaged or lost badge that is three or more years old. In these instances, a photo appointment must be scheduled, and the badge will be replaced at the time the photo is taken.

4.5 Obtaining Temporary, Escort-only and Visitor Security Badges

4.5.1 All temporary, escort-only and visitor security badge requests must be accompanied by the required UW-IT form, available from DCFM Access Control. Applicants must present government-issued photo identification to DCFM Access Control, and allow for the verification of the name and identity of the badge holder.

4.5.2 For all temporary security badge requests, the existing, approved access of the badge holder will be assigned to the temporary security badge. Temporary badges are activated for a 24-hour period. Requests for extensions will be reviewed on a case-by-case basis.

4.5.3 Temporary, escort-only and visitor security badges are only available for issue Monday – Friday, during business hours of the DCFM Access Control office. Contact the DCFM Access Control office at (206) 221-4545 to make arrangements for temporary badges, escort-only and visitor security badges.

4.5.4 All visitors and escorts must fill out the required fields on the visitor and escort sign-in form located in the DCFM Access Control office prior to obtaining the security badge.

4.6 Deactivation and Return of Security Badges

4.6.1 Badge Deactivation: Any change in a badge holder’s status must be reported to DCFM Access Control. If a badge holder no longer requires access to a UW-IT centrally managed data center due to a change in status, DCFM Access Control will immediately deactivate the badge or submit a request for badge deactivation to the leased data center.

4.6.2 Badge Return: Security badges for access to a UW-IT centrally managed data center are property of the University of Washington and must be returned to DCFM Access Control upon deactivation due to changes in the badge holder’s status. Examples of status changes include, but are not limited to: termination of employment, termination or expiration of contractor agreement, retirement, extended family leave, or transfer to another UW department.

4.7 Maintenance of Security Badges
4.7.1 Security badges must not be altered or defaced in any way. Badge holders must not bend the badge, write on or affix anything to the badge, or punch holes in the badge.

4.8 Badge Audits and Access Reviews

4.8.1 Badge audits and access reviews will be conducted by DCFM Access Control according to a predetermined schedule, based on the badge type:

A. UW Employees
   i. UW-IT permanent employees: At any change in status
   ii. UW permanent employees: Annually (every twelve months)
   iii. UW temporary or hourly employees: Semi-annually (every six months)
   iv. UW student employees: Quarterly (every three months)

B. Co-Location Customers and Co-Location Contractors: Annually (every twelve months)

C. Contractors: Semi-annually (every six months)

4.8.2 Notification Date: Upon issuance of a badge, a notification date and time will be entered into the DCFM Access Control database, indicating the due date of the review process.

4.8.3 Badge Extension and Access Review: DCFM Access Control will send notice to the badge sponsor no later than two weeks prior to a badge expiration date. The sponsor must confirm that the badge holder continues to need access, and that the badge continues to be in his/her possession. The sponsor must respond before the badge expiration date. If no response is received, the badge will be allowed to expire.

4.8.6 Access Extension and New Notice: After receipt of confirmation from the badge sponsor, DCFM Access Control will extend access for the badge holder and set new expiration and notification of review dates accordingly.

4.8.7 Loss of Badge/Replacement Badge: If the badge sponsor cannot confirm that the badge holder still retains possession of the badge, access will be discontinued immediately. Upon request from the badge sponsor, DCFM Access
Control will issue a replacement badge, and set new expiration and notification of review dates accordingly.

4.8.8 Sign-in/out Registry Form: All non-UW-IT personnel including but not limited to contractors, co-location customers and others who have authorized access into the data centers must fill out all of the fields on the sign-in/out registry form provided by DCFM Access Control. This sign-in/out registry form will be located just outside the entry door or just inside the entry door. This form will be replaced every month and the old form placed in the DCFM Access Control office and available for the University’s annual audit.

4.9 Security Badge Visibility and Assignment

4.9.1 Security badges must be worn with the photos visible to others at all times.

4.9.2 A security badge assigned to an individual is nontransferable and may not be used by anyone other than the assigned badge holder.

4.9.3 Authorized persons must enter the data center one at a time, and each authorized person must present their security badge to the badge reader in order to log their entry. As a security precaution, everyone entering or leaving a data center should verify that the door is secured. This will help ensure no unauthorized persons enter the room.

5.0 UW-IT–Managed Leased Data Center Security Badges

5.0.1 All personnel entering a UW-leased data center must display a security badge issued by the leased data center and must have been granted access by DCFM Access Control and the appropriate leased data center management.

5.0.2 In order to obtain a security badge or access card for a UW-leased data center, the requestor must possess a current UW-IT security badge, or must have obtained approval for a security badge from the badge sponsor and a UW-IT authorizer. The requestor must submit a badge request form to DCFM Access Control, along with an additional site-specific access request form for each leased data center they apply for.

5.0.3 Once the request has been processed by both DCFM Access Control and the leased data center authority, DCFM Access Control will contact the requester to schedule an appointment for a badge photo and badge issuance at the appropriate UW-leased data center office.
5.0.4 All personnel including visitors, vendors, contractors and UW-IT staff having authorized access into a leased data center facility must sign in and out of the sign-in/out registry form. This form can be provided by the leased facility or by the DCFM Access Control office. This sign-in form will be maintained by the leased data center management and a copy must be provided to DCFM Access Control on a monthly basis for the University’s annual audit. This sign-in/out registry form will be located just outside the entry door or just inside the entry door.

6.0 Unauthorized Photographic Equipment

6.0.1 Cameras or any photographic equipment, including cell phone cameras, are not allowed within any UW data center, network routing center, or UW-leased space containing operational computing, telecommunications or network equipment.

6.0.2 Exceptions to this policy will be evaluated on a case-by-case basis, and any granted exceptions will require preauthorization by a UW-IT unit head (or the unit head’s designee). In such an instance, all photographs must be reviewed and approved by the DCFM Manager prior to leaving the facility.

7.0 UW-IT Data Center Tours or Site Visits

7.0.1 Approval Process: Tours and site visits to a UW data center are granted only under limited circumstances. All tours and site visits must be pre-approved by a UW-IT unit head (or their designee). Requests for site visits or tours of a UW data center must be submitted in writing to the DCFM Manager with a copy sent to DCFM Access Control. The DCFM Manager will review the request and send it to the unit head for approval. All requests must include the following:

A. Reason for visit
B. Number of visitors
C. Name of visitor’s company or organization
D. Day/time of visit

7.0.2 Escort Assignment: Upon approval of a request, an escort from UW-IT’s DCFM group will be assigned to lead the tour or site visit.

7.0.3 Visitor Security Badges: All visitor security badges will be signed in/out at the DCFM Access Control office. A visitor badge must be visibly worn by each guest for the duration of their visit to any campus UW-IT centrally managed data center. DCFM Access Control will assign visitor security badges before a tour or
site visit commences. Information on obtaining visitor security badges can be found in Section 4.5. A UW-IT-issued visitor badge is not required to enter a UW-leased data center when escorted by an approved badge holder. All visitors must sign in and sign out at the security register located at the entrance to each space in accordance with Section 5.0.4.

8.0 Conduct of Authorized Users

8.01 No food or drink is allowed within the data centers and mission critical facilities unless the data center or mission critical space is your duty station and you cannot be relieved to eat or drink outside the data center or mission critical space.

8.02 Authorized users may not tamper or interact with equipment or cabinets that are not assigned to them.

8.03 Customers who purchase shared server cabinets will not tamper or interact with other customer’s equipment housed in the same cabinet. If a major reconfiguration is required by either customer, the work must be coordinated with, and approved by, the UW Information Technology’s Data Center Planner.