ITU Aquia Data Center Access
Process and Procedures for Secure Areas

Purpose

The following procedure is to be followed to limit physical access to critical systems and services which the Information Technology Unit (ITU) has identified. These systems and services are maintained by the Technology Systems Division (TSD) located in the Aquia Building. Specific systems listed in the ITU’s Business Impact Analysis and Risk Assessment for Information Assets are maintained in these secure areas. The procedure provides guidance in obtaining access, reviewing access, and authorizing access to these secure areas.

Facilities – Secured Restricted Areas

The following areas in the Aquia Building have been identified as critical security points and are controlled by swipe card locks managed by the Aquia Data Center ITU.

<table>
<thead>
<tr>
<th>Area</th>
<th>Responsible Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aquia Data Center – Room 114</td>
<td>Aquia Data Center Manager(DCM)</td>
</tr>
<tr>
<td>Aquia Data Center</td>
<td></td>
</tr>
<tr>
<td>Configuration/Storage – Room 110</td>
<td>Aquia DCM</td>
</tr>
</tbody>
</table>

** The Technology Support Services (TSS) Director will be the alternate contact should the Aquia Data Center Manager be unavailable.

Access to the Aquia Data Center requires completion and submission of the “Data Center Access Request Form” to the ITU Aquia Data Center Manager and authorization from the requesting person’s supervisor. The DCM is responsible for maintaining all data center access information.

Access Process Description

Each ITU staff member authorized access to the Aquia Data Center will be registered in the swipe card system and will receive a permanent unique access code that will be associated with their ID. The code is entered in conjunction with the swiping of the Mason ID card for access. The code is not to be shared under any circumstances.

Each ITU staff member authorized access to the Aquia Data Center’s Configuration/Storage, Room 110, currently will only need their Mason ID card for swipe card access.
Non ITU staff requiring access will not be issued swipe card access but will be granted access through a different process explained in the next section of this document.

**Request for Access Process**

Only full time ITU Mason employees are authorized swipe card access to the data center areas.

**ITU Staff**

ITU managers, who have staff requiring regular access to an Aquia Data Center area for their job responsibilities, are to make a request to the DCM for access. The DCM will provide the required Data Center Access Request Form for the requestor to complete and submit for the desired access.

**Non ITU Customers**

Non ITU customers who use physical data center services (equipment hosting) are required to provide an authorized staff listing of individuals needing routine access to the DCM. {Normally part of any Service Level Agreement (SLA) for data center services}

On all visits, the authorized staff member(s) will be logged in by the data center staff prior to access being granted. Only authorized individuals are allowed to sign in visitors that are there to assist them with their equipment. Non ITU customers with authorized access and their visitors are restricted to the area of the data center where their equipment is located during all visits.

Prior to the granting of access, all non full time Mason employees or students requiring regular access to the data center in order to maintain their department’s hosted equipment must have a background check completed by Mason’s Human Resources Department (HR). Requests for the necessary background checks are to be handled by the department’s management through HR. The ITU will not be involved in the details of any results of a background check except for whether an individual was cleared or not by HR prior to their addition to an authorized access list.

The DCM will review all requests for access to determine if all required documentation has been received, all required information is complete, and the requested access is necessary or if the level of access is appropriate.

Once the access has been established for an applicant, the DCM will notify that person and provide them with any necessary access information. In the event that the applicant’s supervisor requests the access information, it will be provided to them in a sealed envelope that is to be given to the employee.
Termination of Access Process

When appropriate for maintaining the physical security of the data center areas, an individual’s access to an area may be removed at any time by request of the person with authority over the secured area or the individual’s supervisor.

Managers are responsible for tracking what Aquia Data Center areas their staff members have swipe card access to and are to notify the DCM if their staff member either departs employment at Mason or no longer requires access.

Individuals whose names are on the Gains & Losses list distributed by Human Resources will have their access removed based on the termination date specified on the list. An individual’s access may also be immediately removed if it is determined that they are violating appropriate access procedures for secured areas.

Aquia Data Center Access Auditing and Review Process

Data Center reports that provide information on each individual with permanent access to the Data Center will be reviewed by the ITU HR liaison, and the ITU Security Office on a quarterly basis, any names on the roster that are identified as not being employed by Mason will have their data center access removed.

A review of the swipe card usage for the Aquia Data Center will be conducted monthly by the DCM to spot check for any suspicious or inappropriate access activity. Any questionable use of access will be investigated and the necessary staff will be contacted to appropriately resolve an incident.

Aquia Data Center reports that provide information on individual access to the data center will be provided to the appropriate ITU Directors and data center customers, for semiannual verification and review.

ITU Directors and the ITU Information Security Officer (ISO) will receive one report semi-annually from the DCM:

- Directors will receive a report with the names of their staff members who have access to the data center. The Director should indicate which employees have left and/or which employees no longer require access to the data center.
- The University ISO will receive a report with the names of everyone with access to the Aquia Data Center

The reports will be returned to the DCM, and he will make appropriate changes to the Aquia Data Center swipe card access system.