Standard: Data Centre & Facilities Access

Effective Date:	2017.02.21
Revision Date:	2020.02.06
Review Date:	2021.02.06
Approving Body:	Director, Information Security and Compliance
Authority:	Information Security Policy
Responsible Owner:	Director, Technology Services
Classification:	Public

Purpose

The University Data Centre and Voice Data Facilities, house systems and equipment critical to the operations of the University of Manitoba and other organizations. This includes, but is not limited to, routers, switches, servers, data storage, voice services, cabling, electrical power and environmental controls. The procedures contained in this document have been developed to maintain a secure environment for these areas, and must be understood and followed by all people, groups, organizations and vendors who are working in, or have systems housed, in these areas.

Who/what does the standard apply?

The requirements in this standard apply to all Data Centre's and Data Facilities managed by the University of Manitoba, including:

- Data Centre's – Fort Garry Campus
- Data Centre's – Bannatyne Campus
- Voice Data Rooms – Fort Garry Campus
- Voice Data Rooms – Bannatyne Campus

Compliance

Data Centre's and Voice Data Room Facilities must align to the requirements and specifications outlined within this standard. Where systems and applications are unable to comply, please submit an Information Security Decision Request to the Director of Information Security and Compliance for review.

Specifications

1.0 Procedure(s)

1.1 Data Centre and Voice Data Facilities Physical Security Procedures

Overview

1.1.1 Security for the University Data Centre and Voice Data Facilities is the responsibility of all groups and organizations that are sharing the space. The Director, Technology Services, is responsible for the administration of these procedures.

1.1.2 The following are the general requirements and practices that govern access to the sensitive areas, for which the Director, Technology Services has responsibility. It is mandatory that all University employees, vendors and organizations with hosted equipment follow these procedures. Any questions regarding these procedures should be addressed to the Director, Technology Services, or their delegate.

Primary Guidelines

1.1.3 The Data Centre and Voice Data Facilities are restricted areas requiring much greater control than normal non-public University spaces. Only those individuals who are expressly authorized to do so by the Director, Technology Services or their delegate, may enter these areas. Access privileges will only be granted to individuals who have a legitimate business need to be in the Data Centre and Data Facilities.

1.1.4 An IST Authorized Access List detailing individuals and their level of access to the Data Centre and Voice Data Facilities will be distributed to the CIO, Director, Technology Services, Director, Information Security and Compliance, Security Services, and the IST General Office on a regular basis (at least annually). A current copy of the IST Authorized Access List, obtained from the Physical Plant Card Access control system, will be kept with the Access Control Log in the Data Centre – for reference.

1.1.5 The only exception allowed to the Data Centre and Voice Data Facilities Access Procedures is temporary emergency access for medical, fire and/or police officials, and University of Manitoba Physical Plant emergency maintenance.

Levels of Access to the Data Centre and Voice Data Facilities

1.1.6 **Controlling Access**: is assigned 24x7 access authority into the Data Centre or Data Facilities. Controlling Access is granted to IST staff whose job responsibilities require that they have access to these areas. These individuals also have the authority to grant **Escorted** and **Unescorted** Access to the Data Centre and Data Facilities and to enable others to enter and leave

the areas. People with Controlling Access are responsible for the security of the areas, and for any individuals that they allow into the Data Centre or Data Facilities. Individuals with Controlling Access normally will be granted access via the Card Access system (card key) and will be placed on the IST Authorized Access List. They must also be prepared to show positive identification at all times in the Data Centre or Data Facilities.

Any individual receiving Controlling Access must have their request approved by the Director, Technology Services.

Individuals granted controlling access may, in addition to the card key access, request key access. However, it is policy of the Director, Technology Services not to issue keys to the Data Centre or Data Facilities for routine access purposes. Requests for this type of access will be considered on a case-by-case, discretionary basis.

Individuals with Controlling Access to the area may allow properly authorized and logged individuals Escorted Access to the Data Centre or Data Facilities.

If a person with Controlling Access allows Escorted Access to an individual, the person granting the access is responsible for escorting the individual granted access and seeing to it they sign in and out. If needed, these duties can be handed-off to another person with Controlling Access on duty in the Data Centre or Data Facilities.

1.1.7 **Escorted Access**: is closely monitored access given to people who have a legitimate business need for infrequent access to the Data Centre or Data Facilities. "Infrequent access" is generally defined as access required for less than 15 days per year.

Individuals with Escorted Access may be issued temporary access cards at the discretion of the Facilities Coordinator and be permitted Unescorted Access for the period of time required to perform scheduled installation or maintenance of equipment. The procedures for Unescorted Access will then apply to this person. The Facilities Coordinator will maintain a log of assigned temporary access cards.

A person given Escorted Access to the areas must sign in and out under the direct supervision of a person with Controlling Access, must provide positive identification upon demand, and must leave the area when requested to do so.

A person with Escorted Access to the areas must not allow any other person to enter or leave the area.

1.1.8 **Unescorted Access**: is granted to a person who does not qualify for Controlling Access but has a legitimate business reason for unsupervised access to the Data Centre or Data Facilities. Examples of this would be an

employee of the University, or employee of an organization with hosted equipment that requires regular access for maintenance. Unescorted Access also includes all members of Security Services, Physical Plant Power Engineers and designated Caretaking staff. Individuals with Unescorted Access to the Data Centre or Data Facilities will be granted access to the areas via card key and will be placed on the IST Authorized Access List.

Individuals with Unescorted Access may either have 24/7/365 access to the Data Centre or Data Facilities, or have access restricted to regular business hours (8:30am - 4:30pm), depending on their business reason. This access will be determined on a case-by-case basis by the Director, Technology Services and recorded on the IST Authorized Access List.

Individuals with Unescorted Access, who require access to the Data Centre or Data Facilities outside regular business hours, must contact Security Services to arrange entry. Security Services is responsible for disarming the alarm and arming the alarm after the work has been completed. Power Plant Engineers are excluded from this contact procedure, which allows them to respond to any alarms or emergencies.

Unescorted Access personnel cannot authorize others to be granted unsupervised access to the Data Centre or Data Facilities. Unescorted Access personnel can only grant escorted access to individuals where related to the grantor's business in the Data Centre. The grantor is responsible for these individuals and must escort them in the Data Centre at all times.

All individuals with Unescorted Access must provide positive identification when asked, and must sign in when entering and sign out when leaving the Data Centre.

1.1.9 Vendor Access to the Data Centre and Data Facilities

The following procedures apply to all outside vendors accessing the Data Centre or Data Facilities.

Regular Hours (Fort Garry Campus) – New Services/Non-Emergency

During regular working hours (Monday – Friday 8:00am – 4:00pm) outside vendors will contact the Data Centre Facilities Coordinator or IST staff member with Controlling Access to schedule an appointment. The Facilities Coordinator or IST staff member with Controlling Access will provided Escorted Access to all contractors working in the Data Centre (E3-625) and 502 Admin. For other voice/data rooms or facilities, the Controlling Access staff member, may grant Unescorted Access and a Temporary Access Card. Access between the hours of 8:00am - 4:00pm Monday to Friday will be provided free of charge. Advance notice is required in order to assure appropriate staff is available.

Regular Hours (Fort Garry Campus) Repair or Emergency Service

During regular working hours (Monday - Friday 8:00am - 4:00pm) outside vendors will contact the Data Centre Facilities Coordinator or IST staff member with Controlling Access to schedule an appointment. The Facilities Coordinator or IST staff member with Controlling Access will provided Escorted Access to all contractors working in the Data Centre (E3-625) and 502 Admin. For other voice/data rooms or facilities, the Controlling Access staff member, may grant Unescorted Access and a Temporary Access Card. Access between the hours of 8:00am - 4:00pm Monday to Friday will be provided free of charge. Every effort will be made to meet the vendor at the required site in a prompt manner. Slight delays will occur in the SmartPark facilities to allow time for the technicians to be transported to the site. Advance notice is preferred whenever possible and allows for shorter response times by the technicians.

After Hours (Fort Garry Campus)

Access after-hours can be arranged but may be a chargeable activity. The vendor may be charged a rate of $60.00 per hour for access after business hours. To obtain access after-hours, outside vendors will contact an IST staff member with Controlling Access or the University of Manitoba Security Services at 474-9312. This line is monitored 24 hours daily/7 days per week. You will be required to leave a phone number and contact name, and will be contacted by appropriate staff to make necessary access arrangements.

Regular Hours (Bannatyne Campus) New Services/Non-Emergency

During regular working hours (Monday - Friday 8:30am - 4:30pm) access to University of Manitoba, Information Services & Technology controlled voice/data rooms can be obtained by contacting a Bannatyne IST staff member with Controlling Access. The IST staff member will accompany all contractors to these rooms or facilities, or if appropriate grant Unescorted Access and a Temporary Access Card. Access between the hours of 8:30am - 4:30pm Monday to Friday will be provided free of charge. Advance notice is required in order to assure appropriate staff is available.

Regular Hours (Bannatyne Campus) Repair or Emergency Service

During regular working hours (Monday - Friday 8:30am - 4:30pm) access to University of Manitoba, Information Services & Technology controlled voice/data rooms can be obtained by contacting a Bannatyne IST staff member with Controlling Access. The IST staff member may request a Bannatyne Security Services (789-3295) or Bannatyne Physical Plant (789-3636) staff member to accompany the vendor. Access between the hours of 8:30am - 4:30pm Monday to Friday will be provided free of charge. Every effort will be made to meet the vendor at the required site in a prompt manner. Advance notice is preferred whenever possible and allows for

shorter response times by the technicians.

After Hours (Bannatyne Campus)

Access after hours can be arranged but may be a chargeable activity. The vendor may be charged a rate of $60.00 per hour for access after business hours. To obtain after hours access, outside vendors may contact a Bannatyne IST staff member with Controlling Access. The IST staff member may request Bannatyne Security Services (789-3330) or Bannatyne Physical Plant (789-3636) staff member to accompany the vendor.

University of Manitoba Statutory Holidays

In the event that access is required on a statutory holiday, the normal access process should be followed. It should be noted that this might also be a chargeable activity at the rate of $60.00 per hour.

Damages to University of Manitoba Property

Should damage result to University of Manitoba property, such as cables, as a result of any vendor's work, the University of Manitoba will invoice the vendor for damages incurred.

Access to rooms and facilities other than those controlled by IST

Access to all other rooms and facilities on campus is covered under the University of Manitoba Physical Plant Policy. If access to an area were required on one occasion, the Physical Plant would arrange for Physical Plant staff to provide access. If a contractor requires ongoing access, Physical Plant would make arrangements for keys to be signed out and returned. No escort will be provided. The exception to this may be the Administration Building. In this case, Security Services may have to escort contractors to the location and remain during access.

Data Centre Doors

1.1.10 All doors to the Data Centre and Data Facilities must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:

a) Allow officially approved and logged entrance and exit of authorized individuals

b) Permit the transfer of supplies/equipment as directly supervised by a person with Controlling Access to the area

c) Prop open a door ONLY if it is necessary to increase airflow into the Data Centre or Data Facility in the case of an air conditioning failure. In this case,

staff personnel with Controlling Access must be present and limit access to the Data Centre or Data Facility.

Security System and Keys

1.1.11 It is the policy of the Director, Technology Services not to issue keys to the Data Centre or Data Facilities for routine access purposes. Requests for exceptions to this policy will be considered on a discretionary, case-by-case basis. If the Director, Technology Services issues a key to an individual, the individual may not share, loan or copy the key. Only those granted Controlling Access can request and be issued keys.

1.1.12 A door code and card access control system provides the normal mechanism for control of access to the Data Centre or Data Facilities. Under no circumstances may an individual attempt to bypass the control system to gain access for them or permit access to another individual. Individuals are not to share their door code or card key.

1.1.13 The Facilities Coordinator, PPEM Card Access Administrator and IST single point of contact for PPEM, perform the actual physical management of keys, card keys and door codes. This includes the actual issuing of keys/codes and maintaining records of key activity.

Periodic Review and Termination/Revocation of Access

1.1.14 Periodic (at least annual) reviews will be performed of those with any level of access to the Data Centre or Data Facilities. The Director, Technology Services will perform these reviews. If an individual no longer requires Data Centre or Data Facilities access, it will be revoked.

1.1.15 The Director, Technology Services will also perform periodic (at least annual) reviews of those with keys to the Data Centre and Data Facilities. If an individual's needs no longer justify a key, it will be collected.

1.1.16 Procedures for terminating and revoking Data Centre or Data Facilities access include:

a) Cancelling door code/card key
b) Collecting key
c) Removing name from the IST Authorized Access List

1.1.17 The results of periodic reviews will be reported to the CIO, IST Directors and Managers, Security Services Director, Facilities Coordinator, and IT Security Coordinator. The report will include the IST Authorized Access List and any names added or removed from that list.

Access Control Log

1.1.18 The Data Centre and Data Facilities Access Control Log must be properly

maintained at all times. The Facilities Coordinator and all individuals with Controlling Access to the Data Centre and Data Facilities are responsible for maintaining this log.

1.1.19 Each time an individual with Escorted Access to the Data Centre or Data Facilities is admitted to the area, he/she must properly log in on the Access Control Log at the time of entrance. The person with Controlling Access to the area who allows the visitor to enter must countersign and fill out the appropriate section of the form.

1.1.20 Each time an individual with Escorted Access to the Data Centre or Data Facilities leaves the area, he/she must properly log out on the Access Control Log at the time of exit (even if only for a short time). The person with Controlling Access to the area who allows the visitor to leave must fill out the appropriate section of the form.

1.1.21 Each time an individual with Unescorted Access enters or leaves the Data Centre or Data Facilities, he/she must properly fill out the Access Control Log.

Requesting Unescorted Access to the Data Centre or Data Facilities

1.1.22 Departments, Organizations or Projects that have systems or equipment in the Data Centre or Data Facilities may request Unescorted Access to the appropriate area. The individuals designated by the requesting Department, Organization or Project will be granted access once the Director, Technology Services authorizes them. To initiate authorization for access, the manager of the group requesting access should direct a request to the IST Facilities Coordinator either in writing or e-mail.

1.1.23 Upon approval by the Director, Technology Services, the IST Facilities Coordinator will set up an appointment with the person requesting access in order to add the person to the IST Authorized Access List and register the person in the security system, if appropriate for the access level granted. At the same time the person will be provided with a copy of the University Data Centre and Data Facilities Access Policy and Procedures documents.

1.1.24 When a person who has access to the Data Centre or Data Facilities terminates his employment or transfers out of the department, as part of the normal exit procedures, the person's Manager must notify the IST Facilities Coordinator as soon as possible so that the person's access to the Data Centre or Data Facilities can be removed. This is extremely important in cases where the employee was terminated for cause.

Escalation

1.1.25 The Director, Technology Services has overall responsibility for the administration of these Procedures. Issues the Director, Technology Services is unable to resolve will be escalated to the CIO or VP Administration, as appropriate.

1.2 Non-Compliance and Reporting Procedures

1.2.1 Persons found to have violated the Data Centre and Data Facilities Access Procedures are subject to University discipline up to and including dismissal and/or any other action in accordance with applicable University governing documents and collective agreements.

1.2.2 Failure of a vendor, consultant, or contractor to follow the guidelines set forth in this document is grounds for termination of agreements and potential legal action.

1.2.3 In cases of financial loss to the University, restitution may be sought.

1.2.4 Ignorance of the Procedures: IST Data Centre and Data Facilities Access Procedures is not an excuse for non-compliance.

1.2.5 To ensure consistency of application, investigation of non-compliance is the responsibility of CIO to coordinate under the authority of the Vice President (Administration).

1.2.6 All infractions of the Data Centre and Data Facilities Physical Security Procedures shall be reported to the Director, Technology Services. If warranted (e.g. emergency, imminent danger, etc.…), Security Services should be contacted.

1.2.7 Any attempt to forcibly or improperly enter the Data Centre or Data Facilities should be immediately reported to Security Services, who should deal with the situation. The senior person present will report the incident in writing to the. Director, Technology Services and Director, Information Security & Compliance.

1.2.8 Individuals with Controlling Access to the area are to monitor the area and remove any individual who appears to be compromising the security of the area or its activities, or who is disrupting operation. It is particularly important that individuals with Controlling Access show initiative in monitoring and maintain the security of the Data Centre and Data Facilities.

1.3 General Data Centre and Data Facilities Operations Procedures

1.3.1 General Hosting Procedure for Data Centre and Data Facilities Capacity Planning

The IST Facilities Coordinator must be consulted for any new equipment to be installed in the Data Centre or Data Facilities. It is advisable to consult with the Facilities Coordinator as early as possible (preferably months before actual equipment is ordered), to confirm your equipment actually can be hosted.

1.3.2 General Procedure on Infrastructure Work in the Data Centre or Data Facilities

The IST Facilities Coordinator must be notified of all work pertaining to infrastructure in the Data Centre or Data Facilities. This includes things such as equipment installation/removal, construction or any activity that adds/removes assets to/from the Data Centre or Data Facilities.

1.3.3 General Safety

All individuals in the Data Centre or Data Facilities must conduct their work in observance with all applicable (i.e. bargaining unit, campus, provincial, federal) policies related to safety.

1.3.4 General Cleanliness

The Data Centre and Data Facilities must be kept as clean as possible. All individuals in the Data Centre or Data Facilities are expected to clean up after themselves. Boxes and trash need to be disposed of properly. Tools must be replaced to their rightful place.

Food and Drink are not allowed in the Data Centre or Data Facilities. The designated office area in the Data Centre is exempt from this restriction.

1.3.5 Procedures for Data Centre Equipment Deliveries and Pickup

A log will be maintained by the Facilities Coordinator that identifies and verifies all equipment that is scheduled to arrive or be picked up from the Data Centre.

The Facilities Coordinator will be responsible for logging all equipment that is scheduled to arrive or be picked up from the Data Centre.

Any department or affiliated organization that is planning to have equipment delivered to or picked up from the Data Centre should contact the Facilities Coordinator and provide details in advance of delivery/pick-up. Please provide the Facilities Coordinator with the following information for the equipment log:

For the delivery of equipment:

a) Expected day of delivery
b) P.O. number for the equipment (if known)
c) Vendor name and description of the equipment
d) Person to be contacted when the equipment arrives

For the pick-up of equipment:

a) Expected day the equipment will be picked up
b) Vendor name, description and location of the equipment to be picked up
c) Name of person to be notified once equipment is picked up

References

Information Security Policy and Procedures	