Server Colocation Standards

1 Overview

The purpose of this document is to communicate the minimum requirements and configuration necessary to colocate a server or other equipment in the datacenter of Duke University's Fuqua School of Business (hereafter noted as "Fuqua"). Fuqua can upon request provide rack space, power, cooling and network connectivity in a secure monitored environment for non-Fuqua owned equipment to meet missions, goals, and initiatives of Fuqua faculty. Only equipment that meet the requirements specified in this document or are granted an exception by the Director of Enterprise Systems and Services are approved for colocation in the Fuqua datacenter.

2 Scope

The terms of this document apply to all faculty and staff (hereafter noted as "client") who colocate equipment in the Fuqua datacenter, including their authorized agents, contractors, consultants, temporary and other workers, as well as any equipment the client colocates in the Fuqua datacenter.

The Director of Enterprise Systems and Services must approve exceptions to this set of standards in advance. This document may be altered or updated at any time at the sole discretion of the Director of Enterprise Systems and Services.

3 Datacenter Environment

3.1 Cooling and air handling – Datacenter humidity, air temperature and ventilation is controlled by two Liebert CRAC units that are maintained by Duke University Facilities Management. Air is generally kept at approximately 70 degrees Fahrenheit and 40% humidity. The CRAC units are on a circuit backed by generator power to maintain service in the event of a power failure in the datacenter or building. Air is circulated under a raised floor and directed at the server racks using perforated floor tiles.

3.2 Power – Power is tempered by a 65 kVA Liebert Npower UPS. The UPS is backed by generator power to maintain service in the event of a power failure in the datacenter or building. The UPS, overhead busways and redundant in-rack PDUs are all monitored and configured to deliver notification if an out of normal range event is detected.

3.3 Network – The datacenter has a redundant 10Gb connection to the greater Duke University network and is bounded by a Fuqua maintained Cisco ASDM firewall. The datacenter itself has 10Gb, 1Gb, and 10/100Mb switches to connect equipment to the network. All connections and equipment that manage or utilize OSI layers 1-4 are maintained and monitored by Duke University OIT-Network Services. Duke University OIT-Network Services also provides DNS services to all clients within the campus network, although Fuqua runs DNS servers as well to resolve internal (Fuqua.duke.edu) addresses.

3.4 Security – In addition to the firewall noted above, Duke University utilizes and maintains the following security services:

- Load-balanced intrusion detection systems that perform packet inspection and filtering.
- Monthly and ad-hoc security and vulnerability scans.
- Log and event monitoring and analysis.
- Anti-virus protection with the client available either as a stand-alone application or managed by a centralized console.

3.5 **Access control –** Access to the datacenter is controlled by an electronically locked door, secured with a badge reader. There is a limited list of authorized badge holders and the list membership, as well as badge usage are reviewed weekly. Active monitoring inside the datacenter provides an additional layer of security.

3.6 **Raised floor –** The datacenter is equipped with a raised floor to circulate conditioned air and direct it to the equipment racks.

3.7 **Fire suppression –** The data center is equipped with a FM-200 fire suppression system.

3.8 **Racks** – The datacenter is equipped with industry standard APC 19-inch (42U) racks and redundant in-rack monitored PDUs.

4 Services Offered

4.1 **Services –** Fuqua will, currently at no cost to faculty members, provide the services listed below. Any required services other than those enumerated below will be considered on a case-by-case basis. Fuqua will, within reason, supply network cables necessary to connect hosted equipment to the Duke University network and the internet at large.

4.1.1 **Colocation of servers** – Fuqua will host faculty owned servers that meet or exceed the requirements enumerated in section 5.2.

4.1.2 **Colocation of non-server rack-mountable equipment** – Fuqua will consider on a case-by-case basis whether it will host faculty owned non-server equipment. In general, any such equipment must meet or exceed the requirements enumerated in section 5.2, wherever those requirements apply to the equipment in question.

4.1.3 **Colocation of racks** – Fuqua will consider hosting faculty owned racks on a case-by-case basis. Any hosted racks must meet or exceed the requirements enumerated in section 5.2.

4.1.4 **Virtual Machines** –Virtual Machines (VMs) can, within reason, be built to the specifications and requirements of the faculty member, and be hosted in the Fuqua virtual environment. Requests to host VMs built, configured or provided by parties outside the Fuqua environment will be considered on a case-by-case basis. All VMs hosted by Fuqua must meet or exceed the requirements enumerated in section 5.2.2.

4.1.5 **Additional Services**

4.1.5.1 All hosted equipment will be located behind Fuqua and Duke University firewalls. Both firewalls are configured for unrestricted out-bound traffic, with in-bound traffic locked down to most common ports and protocols. Permission for non-standard port inbound access will be considered on a case-by-case basis.

4.1.5.2 The Duke University IT Security Office (ITSO) performs regular vulnerability scans of all Duke public subnets. All hosted equipment that is assigned a public IP address will be included in these scans.

4.1.5.3 “Remote hands” service can be provided during regular business hours (Monday through Friday, 8 am to 5 pm, University holidays excluded) with 4 hours advanced notice.

4.1.5.4 Requests for support should be routed through the Fuqua Technical Support Center. A member of the Infrastructure team is on-call 24 hours a day, 365 days a year to respond to emergency situations involving systems classified as Mission Critical Production.

4.2 **Limitations**

Limitations to services provided by the Fuqua Infrastructure Team (hereafter noted as "provider") include, but are not limited to the following:

4.2.1 The provider is not responsible for damage caused to equipment incurred through improper packing, delivery, installation or removal of equipment unless these activities were performed by the provider.

4.2.2 The provider reserves the right to perform a security scan on any equipment the client submits for colocation that is not delivered in factory sealed packaging**.**

4.2.3 Any movement of hosted equipment within the datacenter is at the discretion of the provider, and will be done in the manner least disruptive to the client whenever possible. The client agrees to coordinate with the provider any placing of new or relocation of existing equipment.

4.2.4 Fuqua has a limited number of IP addresses in public and private ranges. Hosted equipment requiring an IP address and needing network access will be assigned an address as available and deemed appropriate by the provider.

4.2.5 Use of a private address does not absolve customer of responsibility for adhering to Fuqua security and maintenance requirements (see section 5.2.1.6 or 5.2.2.1).

4.2.6 DHCP services are not provided by Fuqua, but may be available from Duke OIT on certain subnets.

4.2.7 The provider reserves the right to block from the network any server that it believes poses a serious threat to campus computing resources or the Internet. This may involve a compromised host or one identified as causing severe performance issues affecting other hosts or subnets**.**

4.2.8 Backup and recovery services are not offered as part of this colocation service but can be negotiated separately.

4.2.9 Use of network attached storage is not offered as part of this colocation service but can be negotiated separately. External data storage capacity is also offered by Duke University OIT.

4.2.10 Power strips are not permitted for use within racks**.**

5 Statement of Requirements

All hosted equipment must meet or exceed the requirements and standards listed below. These include, but are not limited to:

5.1 General Requirements

5.1.1 The client must not change the network configuration of their equipment without prior consultation with the provider. Any changes that affect the accuracy of labeling must be accompanied with the updating of such labeling.

5.1.2 Duke University and the provider perform regular maintenance on datacenter systems and infrastructure, and some of these activities may affect the accessibility or performance of client equipment. The provider will make reasonable efforts to provide the client with advanced notice of these activities. The client assumes responsibility for being aware of these notifications and for contacting the provider with any concerns related to maintenance activities.

5.1.3 The client is responsible for staying in compliance with all Duke University security standards (http://security.duke.edu/policies-procedures).

5.2 Requirements for Equipment

5.2.1 Physical Equipment and Servers

5.2.1.1 Any cabling or cords belonging to the customer must meet datacenter minimum standards and be properly wrapped, secured, and labeled (both ends) in accordance with datacenter standards.

5.2.1.2 All hosted equipment must have redundant power supplies and must come with its own power cords. Power cords for in-rack equipment must have an IEC C14 connector on the end to be plugged into the in-rack PDU.

5.2.1.3 All servers must be rack-mountable and must come with a rack-mount kit.

5.2.1.4 All servers must have a functioning Out-of-Band management system (also known as Lights-Out, or Remote Lights-Out).

5.2.1.5 All hosted equipment must meet established industry electrical, thermo, and magnetic standards. The provider will request removal of any equipment out of compliance with established standards.

5.2.1.6 The client is required to maintain host-based firewall software properly configured to limit access to only necessary ports and protocols, to use and keep current ITSO approved anti-virus software when available, and to keep current with server software patches. All colocation clients must adhere to these Standards. In the event of an emergency the provider must be notified immediately.

5.2.1.7 Client equipment or peripherals may not block or impede access to Fuqua equipment.

5.2.1.8 Client equipment will be labeled by the provider in accordance with Fuqua datacenter standards.

5.2.1.8 All client owned equipment must be removed from the datacenter within 60 days of termination of any colocation agreement. Any equipment remaining after this time is subject to disposal through the Duke Asset Disposal System.

5.2.2 **Virtual Servers**

5.2.2.1 The client is required to maintain host-based firewall software properly configured to limit access to only necessary ports and protocols, to use and keep current ITSO approved anti-virus software when available, and to keep current with server software patches. All colocation clients must adhere to these Standards. In the event of an emergency the provider must be notified immediately.

5.2.2.2 While the client is responsible for maintaining the operating system and software installed on their server, VMs require certain configurations to operate properly in a virtual environment. The provider must be able to install virtualization management software and retains the right to manage hosted VMs as necessary to maintain the performance, stability, and security of the overall virtual environment.

5.3 Requirements for Equipment Owner and Their Authorized Agents

5.3.1 The client is responsible for any costs or expenses related to equipment delivery or removal. The client is also is responsible for all costs and expenses associated with installed devices and peripherals, software, maintenance and associated vendor relations**.**

5.3.2 Delivery or pick-up of equipment must be coordinated with the provider. Failure to coordinate with the provider may result in refusal of delivery or pick-up.

5.3.3 Any equipment requiring addition, alteration or upgrade of any datacenter equipment, infrastructure or resources must be reviewed and approved by the provider. Requests to accommodate such equipment may be denied at the discretion of the provider.

5.3.4 The client is responsible for administering, managing and troubleshooting all hardware, operating systems and applications on hosted equipment. Administration by the provider is generally not offered but may be considered on a case-by-case basis.

5.3.5 The client must make available to the provider credentials or other access methods to hosted systems that will grant the provider administrative control of said systems. The provider warrants that provided access will be used only as required to perform actions and services either explicitly requested by the client, or required for the stability and security of the Fuqua IT environment.

5.3.6 The client is responsible for storage of operating system and application installation media or source code.

5.3.7 The client must ensure that system and security contact information is kept up-to-date.

5.3.8 If any vulnerabilities of severity “Critical” or “High” are discovered during an ITSO vulnerability scan (as noted in section 4.1.5.2), the client must remediate the vulnerability within two weeks of notification by the provider. Vulnerabilities of severity “Medium” must be remediated within 60 days of notification by the provider. Client requests for assistance with security issues will be considered on a case-by-case basis. The provider may, at its discretion, remove the vulnerable node from the network if remediation is not completed within the notification time specified.

5.3.9 The client must provide advanced notification (2 business days) of planned maintenance that requires physical access to colocated equipment. The client agrees to coordinate such access with the provider. If maintenance will require non-Fuqua personnel to enter the datacenter, the client agrees to supply the provider with contact information and credentials of the non-Fuqua maintenance provider. All persons entering the datacenter

must be accompanied by a member of the Fuqua Infrastructure Team. Notification by the client to the provider of planned maintenance is not a guarantee that access will be provided. Work space must be left in the same condition in which it was found.

5.3.10 The client or their authorized agent may only access racks that contain their equipment, and may only access their own equipment in the racks.

5.3.11 The client agrees not to use colocated equipment in ways that negatively impact other equipment in the datacenter, its infrastructure, network, or other resources.

5.3.12 The client agrees not to use their equipment to conduct illegal activities or for storage of illegal materials. Violation of this provision may result in immediate termination of colocation agreement and any equipment used for such activates may be confiscated or delivered to law enforcement agents as stipulated by legal requirements.

6 Rules within the Datacenter

Anyone entering the Fuqua datacenter must adhere to the following rules:

- No food or drink is allowed within the datacenter.
- No weapons or hazardous materials are allowed within the datacenter.
- All packing material must be removed from the datacenter at the time of equipment installation.
- No cleaning supplies (including water) are allowed within the datacenter.
- Doors are not to be propped, blocked or taped open.
- Customer or their agent may not use compressed air on their equipment without prior consultation with the provider.
- Photographs or video recordings are not allowed within the data center without prior approval.
- Floor tiles must be removed and replaced by the provider only, or their authorized agents.

7 References

In support of this standard, the following policies, guidelines, and resources are included:

- Duke University IT Security Office Policies and Procedures.
- Fuqua School of Business IT Security Policies

8 Definitions

Term	Definition
Busway	A conduit for electrical power distribution.
Colocate, colocation	Placement or hosting of equipment from multiple owners in a shared environment.
CRAC	Computer room air conditioning unit. Maintains air temperature through heating or cooling, stabilizes environmental humidity, and distributes conditioned air in the datacenter.
Datacenter	A facility to house computer systems and electronic equipment that provides reliable and stabilized power, environmental controls, connectivity, and security to support business functions and continuity.

DHCP	Dynamic host configuration protocol. A system for automatically assigning IP addresses and network configuration to allow computers to communicate on a shared network.
DNS	Domain naming system. The system that allows network connected devices to recognize and interpret host and domain names on a network or the internet.
Emergency	Any event or condition that impedes, disrupts, harms, or threatens imminent disruption or harm of normal business operations, or the systems that facilitate normal business operations.
Firewall	A physical or logical device that evaluates and regulates network communications for compliance or violation of configured rules relating to such communication.
IEC C14	An industry standard design for power cord termination.
ITSO, Duke University ITSO	Duke University's Information Technology Security Office.
OIT, Duke University OIT	Duke University's Office of Information Technology.
OSI (layers)	Open Systems Interconnect, from the OSI Model that defines functions of a communications system by separating it into layers[1]. OSI layers 1 – 4 generally describe the physical components required for computer network communications, along with the protocols used for this communication.
Out-of-Band management system	Also known as Lights-Out or Remote-Lights-Out, or by a proprietary name such as DRAC (Dell Remote Access Card) or ILO (HP Integrated Lights-Out). A technology for accessing and controlling a computer from a remote location. Allows for remote access to the console session of the computer operating system, as well as the ability to remotely power-on the computer and interact with the boot process.
PDU	Power Distribution Unit. An in-rack component that distributes and tempers power used by racked equipment. Many PDUs also provide for local and remote monitoring of power distribution, as well as the ability to remotely control individual outlets on the PDU.
Remote hands	On-site hands-on work to be done on hosted equipment by the provider at the client's request.
Severities Critical, High, Medium	Severity levels of detected vulnerabilities are scored according to standards defined in the Common Vulnerability Scoring System (CVSS) developed by the National Infrastructure Advisory Council (NIAC). These severity levels indicate the level of urgency perceived in relation to the vulnerability and the risk and potential damage that may be incurred if the vulnerability is not remediated.
UPS	Uninterruptable Power Supply. A device that sits between the source of power entering the datacenter and the equipment housed in the datacenter. The UPS tempers incoming power to even out fluctuations that may cause performance degradation, monitors the strength and consistency of incoming power to rapidly detect drops or spikes in voltage or failure of power, and stores large amounts of power to maintain datacenter functions when a power failure occurs. This last function allows for a

[1] This definition was adapted from Wikipedia: http://en.wikipedia.org/wiki/OSI_model

	temporary continuation of function until normal power is restored or until generator power comes on-line, and also allows for graceful shutdown of resources if no reliable source of power is available.
Virtual server, VM	A logical or "virtual" abstraction of a server. A VM acts like and does the work of a physical server but is not directly dependent on a specific hardware platform.
Virtual environment	An organized logical or programmatic container for Virtual Servers and resources that facilitates configuration, management and control of the VMs and resources it contains.

9 Revision History

Date	Who made the revision	Change made
2014-08-12	Seth Waller	Initial issue
2018-03-28	Seth Waller	Edited section 5.2.1.2 to reflect the requirement for redundant power supplies.