Data Center Work Rules
SV1-FAC-FPO-MGT-1427

Policy

1.0 RESPONSIBILITIES:

1.1 It is the responsibility of all contractors to comply with this policy.

1.2 It is the responsibility of the Project Manager to ensure that all contractors are aware of, understand, and have been trained on the Data Center Work Rules and requirements.

2.0 PROCESS OVERVIEW AND POLICY

2.1 All contractors must be trained and display an understanding of the Data Center Work Rules. Contractors will adhere to the rules and guidelines set forth by the Facilities team at all times while on the premises.

2.2 All contractors must pass a written exam demonstrating that they have read and understand the contents of this document. A passing score is 70%.

2.3 Contractors who complete orientation and pass the written exam will receive a certification good for one year from the completion date.

2.4 Upon expiration of certification the contractor will be asked to review the Data Center Work Rules making note of any changes in policy and take another written exam.

3.0 GENERAL WORK RULES

3.1 PERSONAL BEHAVIOR

3.1.1 All vendors, contractors and other service providers must be appropriately attired and act in a professional manner.

3.1.2 No firearms, explosive chemicals or devices, or weapons of any type are allowed on the site.

3.1.3 Smoking is not allowed inside the building.

3.1.4 Profane language, abusive behavior, being under the influence of alcohol or drugs, sexual comments to or about employees, leering, and other offensive or inappropriate behavior will not be permitted and offenders will be asked to permanently leave the premises.

3.1.5 Personal entertainment devices (Radios, MP3 players, etc.) are not permitted in Data Center.

3.1.6 No food or drink is allowed on the raised floor space. Food and drink is permitted in designated locations only.

3.2 SAFETY

3.2.1 Be safe!

3.2.2 When in doubt, ask!

3.2.3 Be sure you thoroughly understand what you are going to do before you proceed. You may not have a second chance to correct a mistake.

3.2.4 When in doubt be conservative!

3.2.5 Obey safety cones, barricades, caution tape, or other safety equipment that has been installed to guide you around hazardous areas.

3.2.5.1 Red tape means DANGER, do not enter for any reason. You must be responsible for a specific task for the work being performed to cross that boundary.

3.2.5.2 Yellow tape means CAUTION, do not enter without permission from the person performing the work. Do not assume a work area is safe.

3.2.6 Contractors will not block access ways unless absolutely necessary to complete their work. If blocking an access way is necessary, the contractor will contact the Facilities Team for approval. Safety cones and/or caution tape will be placed around the work area when access ways are blocked.

3.2.7 Emergency evacuation routes, including stairways and exit doors, are never obstructed or blocked.

3.2.8 Raised or uneven floor surfaces and other physical obstructions that may pose a tripping hazard are identified using cones or other appropriate warning devices to inform others of the hazard.

3.2.9 In the event of a fire alarm, all employees, vendors, and contractors are to evacuate the building immediately. Foremen or lead persons are responsible for checking worker headcount and reporting to the fire official in charge that their people are out of the building. Do not leave the premises until you have been accounted for and have communicated your departure to your foreman or lead person.

3.2.10 In the event of physical injury, please notify your Project Manager or Security personnel immediately. In an emergency call 911 or notify Security to do so.

3.2.11 Follow proper ladder safety guidelines.

3.2.12 Carrying awkward loads within the Data Center requires a minimum of two people (one on each end).

3.2.13 Contractors using hand and power tools and exposed to falling, flying, abrasive, and splashing objects, or exposed to harmful dust, fumes, mists, vapors, or gases are responsible to have and wear the proper PPE (Personal Protective Equipment), such as safety glasses, face shields, protective gloves, etc.

3.3 Hazardous Materials

3.3.1 Materials deemed hazardous must be in an acceptable container, approved by the Facilities Manager, and accompanied with a Material Safety Data Sheet (MSDS) and a copy posted in the MSDS binder in the front lobby.

3.3.2 Paints, solvents, adhesives, or any other flammable materials must have the approval of

the Facilities Manager before they are brought inside the data center. These must be kept to a minimum, and may not be stored in the Data Center. These are considered hazardous materials and must be accompanied by a MSDS.

3.3.3 All solvent waste or flammable liquids, leftover paint, cleaners, oily rags and other cleanup materials, and other materials are to be kept in properly labeled, fire resistant, closed containers until removed from the Data Center.

3.3.4 Chemical wastes are to be disposed by the Contractor in strict compliance with applicable government regulations.

3.3.5 All spills of materials deemed hazardous must be reported immediately to the Facilities Team. Spills of certain types of hazardous materials require immediate reporting by SAVVIS to governmental agencies. Contractors are to consider any chemical spill as a serious event.

3.3.6 A Contractor violating this policy will be permanently barred from the premises.

3.3.7 A Contractor attempting to "cover up" a chemical spill may be subject to legal action by governmental agencies.

3.3.8 Always make sure you are aware of the location of the fire exits as well as the nearest fire extinguishers. Evacuation maps are posted throughout the Data Center.

3.3.9 In the event of a fire, earthquake, or other life threatening emergency all employees, vendors, and contractors are to evacuate the building immediately. Do not leave the premises until you have been accounted for and have communicated your departure to your foreman or lead person.

3.3.10 Foremen or lead persons are responsible for checking their worker headcount and reporting to the fire official in charge that their people are out of the building.

3.3.11 In the event of a medical emergency call 911 or notify SAVVIS Security to do so. Remain with the injured person until help arrives.

3.4 WORK SITE CLEANLINESS

3.4.1 It is the responsibility of the contractor performing work on the premises to keep the work site clean and free of hazards.

3.4.2 Contractors will not block access ways unless absolutely necessary to complete their work. If blocking an access way is necessary, the contractor will contact the Project Manager for approval. Visual barriers will be installed when access ways are blocked.

3.4.3 Contractors will not block airflow in the data center with equipment, carts, doors, etc. unless absolutely necessary to complete their work. If blocking airflow is necessary, the contractor shall contact the Project Manager for approval.

3.4.4 To limit the amount of airborne particles, all vacuums used in the data center will have a HEPA discharge filter capable of limiting discharged particles to 0.3 microns.

3.4.5 Liquids are not allowed on the raised floor areas unless absolutely necessary to complete the required work and are approved by the Project Manager.

3.4.6 All packing material must be removed from equipment and components in the specified staging areas before being moved onto the Data Center floor.

3.4.7 Storage of tools and equipment in the Data Center is not desirable and shall only be done with the permission of the Project Manager.

3.4.8 Work areas must be clean prior to contractors and vendors leaving for the day and/or upon the completion of the job.

3.5 CONTROL OF EQUIPMENT AND STOP WORK AUTHORITY

3.5.1 **Any** person in the data center, including a customer, has the authority to stop work.

3.5.1.1 Upon being issued a stop work order by one of these staff members, the contractor must immediately place the work area in a safe condition and stop work.

3.5.1.2 The contractor should immediately contact the Project Manager for guidance.

3.5.1.3 Any worker found in violation of a stop work order can be permanently barred from the site.

3.5.2 All equipment at this site is under the control of the Facilities Team. If work is to be accomplished on equipment, the Facilities Team must turn over control of the equipment to the contractor/workers before work can be accomplished.

3.5.3 When work has been completed, the contractor/worker must turn over control of the equipment to the Facilities Team prior to leaving the work area or they will be called back to do so.

3.6 FIRE DETECTION AND SUPPRESSION SYSTEMS

3.6.1 Pre-action water sprinklers protect under and above the raised floor and above office and support spaces. The sprinklers will function automatically when a temperature exceeds a preset level and the fire detection system is in alarm. Every effort shall be made to prevent such a condition from ever occurring.

3.6.2 On activation of a smoke detector intense flashing strobe lights will flash and horns will sound.

3.6.3 In the event of a fire alarm, evacuate the Data Center immediately. Go directly to the nearest safe exit unless directed otherwise by Security personnel.

3.6.4 Never prop open a fire rated door. Leaving doors open degrades the survivability of the building and affects computer room temperature, humidity, stability and security.

3.6.5 A fire watch will be established any time a fire detection alarm or suppression system is disabled. A fire watch requires a complete physical tour of all spaces in the de-activated fire detection zone at least twice every hour. Technicians will not be permitted to leave the site until all fire systems have been re-enabled or the Project Manager has assumed responsibility for another project in work.

3.7 EMERGENCY POWER OFF (EPO)

3.7.1 EPO buttons are located at the exits on each floor and are carefully labeled. Operation of

an EPO button removes all power within a particular computer room zone and results in a failure of the Data Center. This is an extremely serious event.

3.7.2 Use the EPO button only in the event of a major life-threatening emergency. If possible and prudent, attempt to localize the problem before using the EPO which shuts off power to an entire computer room and has a major impact on the entire company.

3.7.3 Operation of the EPO button requires pressing two individual buttons. An alarm will sound when each button is pressed. Do not press the reset button on the EPO panel. Only qualified Facilities personnel with the approval of Facilities Management can reset an EPO panel.

3.8 DATA CENTER ACCESS

3.8.1 Access

3.8.1.1 The Project Manager must be notified and approve arrival or departures of contractor personnel. Security will notify the Project Manager listed on the work order upon contractor check-in.

3.8.1.2 A valid Work Order is required to gain access to the data center to perform work. The contractor must specify what work order he/she will be working on during that visit.

3.8.1.3 A Siebel ticket must be opened for access to an occupied cage. The Siebel ticket number must be included on the approved work order. The project manager will make sure the Siebel ticket gets generated and listed on the work order. Only Security personnel are allowed to unlock an occupied cage for a contractor to perform work.

3.8.1.4 The Project Manager must be notified before moving large equipment into or out of the building, or the main computer room, or from the dock area so open doors and door alarms may be managed.

3.8.2 Keys/Access Cards

3.8.2.1 Contact the Project Manager to access any secured areas such as the roof, equipment rooms, storerooms, equipment, power panel etc.

3.8.2.2 Keys and/or key rings never leave the building.

3.9 REQUIREMENTS FOR WORKING IN THIS SITE

3.9.1 All work will take place within the date range on the work order and in accordance with the Project Manager's communicated schedule. Vendors and contractors are required to contact the Project Manager upon arrival to the Data Center and before any work is performed.

3.9.2 Pre-plan the tools and materials required for each day's work.

3.9.3 Do not set things on top of equipment or block access to any aisle ways, doors, air conditioning or Power Distribution Units, EPO or electrical panels.

3.9.4 Use safety cones, barricades, caution tape, or other safety equipment and devices to direct

people away from hazardous areas. Replace all floor and ceiling tiles before breaking for lunch and at the end of each day.

3.9.5 Do not cross protective barriers or devices without asking permission from the person performing the work. Be especially aware in areas where floor tiles can be removed exposing the under-floor area.

3.9.6 In the event of an audible alarm or unusual noises on any piece of equipment in the Data Center, please contact your Project Manager or a Security Officer immediately.

3.9.7 The dock area is for unloading only - no parking is permitted. Vendor trucks are to be parked in the locations specified by the Project Manager.

3.9.8 All packing material must be removed from equipment/components in the specified staging areas before being moved onto the active raised floor.

3.9.9 Storage of tools and equipment in the data center is undesirable and should only be done with the permission of the Project Manager. When storing tools and materials in the data center, store them neatly in an area approved by the Project Manager.

3.9.10 Removal of raised floor tiles or ceiling tiles must be authorized by the Project Manager, (see section 12).

3.9.11 Materials deemed hazardous must be in an acceptable container, approved by the Facilities Manager, and accompanied by an MSDS sheet before being brought into the data center. A copy of the MSDS sheet must be placed in the MSDS binder in the front lobby.

3.9.12 Paints, solvents, adhesives, or any other flammable materials must have the approval of the Facilities Manager before they are brought inside the data center, must be kept to a minimum, and may not be stored in the building. All hazardous materials must be accompanied with a Material Safety Data Sheet (MSDS) and a copy posted in the MSDS binder in the front lobby.

3.9.13 Contractors may only use electrical outlets marked "House Power" for their power tools.

3.9.14 Put things away at the end of the day.

3.9.15 Penetrations to rated firewalls or smoke barriers must be maintained on a daily basis.

3.9.16 Workers shall not leave at the end of the day or job until the Facilities Engineer has released them, their work area is clean and safed-off, and they have signed out via the logbooks in the lobby.

3.9.17 Contractors must sign in and out on the “contractor” sign-in sheet in the lobby. Do not sign the “customer” sign-in sheet.

3.10 INITIATING A PROJECT

3.10.1 All work must have a written Work Order. Verbal or hand written instructions are not allowed. The work order will contain the task instructions or reference other approved procedures.

3.10.2 All procedures will be reviewed and agreed upon by the contractor before work begins. Any questions or concerns shall be communicated to the Project Manager.

3.10.3 Any deviations from the approved work scope or procedure shall be evaluated and approved by Facilities Management prior to work start.

3.10.4 The contractor shall check off steps in the work procedure as he/she completes them to avoid skipping a step or performing steps out of sequence. The contractor shall be able to provide status at any time during the task if asked to do so.

3.11 CLOSING OUT A COMPLETED PROJECT

3.11.1 Work must be done to the satisfaction of the Project Manager. The contractor shall contact the Project Manager to review the work for buy-off.

3.11.2 All temporary or interim solutions must be removed, all penetrations must be permanently sealed, tools and materials must be removed, and as-built documentation must be completed.

3.11.3 Work area must be cleaned.

3.11.4 The work order, procedures, and drawings shall be returned to the Project Manager with comments and redlines.

3.12 ESSENTIAL DOCUMENTS FOR WORKING IN THE FACILITY

3.12.1 Work Order. There must be a Work Order established prior to data center access.

3.12.2 Approved Procedure. The approved procedure must be "at hand" in the work area and visible where critical work is being performed. Work will be immediately halted if the approved procedure is not available or is not being followed.

3.12.3 Drawings and Layouts. All construction projects should be accompanied by revised drawings or layouts showing the intended configurations.

3.12.4 Welding and Cutting Permits. No welding or open torches will be used without a permit and without disabling the fire detection and suppression systems in the zone affected.

3.12.5 Materials Safety Data Sheet (MSDS). Provide a Materials Safety Data Sheet for any material you bring into the facility. The MSDS binder is located in the lobby and will be maintained by the Facilities Manager.

3.12.6 Level of Readiness Checklist. Before beginning work, make sure that all LOR checklist items have been addressed.

3.12.7 Panel Schedule. If you are working on customer circuits you must have an updated panel schedule.

3.12.8 Other documents may be required depending upon the work to be performed.

3.13 GENERAL WORK RULES

3.13.1 Be especially careful around any computer hardware that has had the protective outer metal skin removed. With its covers off, such equipment is usually more susceptible to nearby electrical disturbances or dust.

3.13.2 Pipe cutting, pipe threading, cement cutting or drilling within the data center requires the

prior approval of the Facilities Manager. .

3.13.3 Any vacuum used in the Data Center must have a HEPA filter. A wet vacuum may be used for water recovery only and with the approval of the Facilities Management.

3.13.4 Gunpowder discharge activated construction tools or devices are not permitted.

3.13.5 All work on the Data Center's critical equipment must follow an approved SAVVIS procedure.

3.14 RAISED FLOOR AND CEILING TILES

3.14.1 To protect the surface and physical strength of the raised floor from heavy computer equipment rolling spot loads, use 3/4" plywood taped with 3" duct tape at all seams.

3.14.2 Tiles have a weight bearing capacity of 300 pounds per square foot. The contractor will identify the weight bearing capacity of the floor tiles prior to moving heavy loads.

3.14.3 Minimize the size of cable cutouts to limit the unnecessary loss of cooling air and static pressure.

3.14.4 Cutouts in floor tiles shall be protected with permanent plastic trim strips.

3.14.5 Replace all previously cut or drilled floor tiles no longer in use with full tiles

3.14.6 Do Not move a perforated floor tile or ceiling ventilation duct without first consulting the Project Manager.

3.14.7 Removing ceiling and floor tiles affects the dynamics of the HVAC system in our data center. With permission from the Project Manager you may remove up to three (3) floor tiles and three (3) ceiling tiles at one time. If it is impractical to perform the work with this limited access, a variance can be given by the Lead Engineer if the level of risk allows. The contractor will contact the Project Manager if a variance is needed.

3.14.8 When removing ceiling and floor tiles, you must use a HEPA vacuum to catch dirt and debris from contaminating the data center.

3.14.9 When removing ceiling and floor tiles, you must first safe off the area with safety cones and or barricades.

3.15 DATA CENTER SECURITY

3.15.1 Contractor personnel must display a Temporary Security Badge at all times. Return this badge to the Security Desk daily.

3.15.2 Contractor personnel must enter the data center through the front lobby and check in with security to obtain their Temporary Security Badge. No one is permitted to enter the data center through an alternate entry point until that person has checked in with Security in the front lobby.

3.15.3 Contractor personnel must sign in and out on the "Contractor" log sheet located in the front lobby of the data center. Do not sign in on the "Customer" log sheet.

3.15.4 The Data Center staff conducts rounds of the building. They are authorized to request seeing SOPs for the work being done. They can order work to be stopped if they feel procedures are not being followed or if any threat to data center stability, safety, or operations exists.

3.15.5 Access

3.15.5.1 All Contractor personnel must present a valid government issued pictured ID when they check in with SAVVIS Security. NO EXCEPTIONS. No Contractor will be allowed access to the facility without presenting identification.

3.15.5.2 The Project Manager must be notified and approve arrival or departures of contractor personnel. Security will notify the Project Manager listed on the work order upon contractor check-in.

3.15.5.3 A valid Work Order is required to gain access to the data center to perform work. The contractor must specify what work order he/she will be working on during that visit.

3.15.5.4 A Siebel ticket must be opened for access to an occupied cage. The Siebel ticket number must be included on the approved work order. The project manager will make sure the Siebel ticket gets generated and listed on the work order. Only Security personnel are allowed to unlock an occupied cage for a contractor to perform work.

3.15.5.5 The Project Manager must be notified before moving large equipment into or out of the building, or the main computer room, or from the dock area so open doors and door alarms may be managed.

3.15.6 Keys/Access Cards

3.15.6.1 Contact the Project Manager to access any secured areas such as the roof, equipment rooms, storerooms, equipment, power panel etc.

3.15.6.2 Keys and/or key rings never leave the building.

3.15.7 Contractors and vendors are granted access into the Data Center to perform specific tasks within a specific area. It is no a license to wander about the Data Center. Many areas within the Data Center are restricted even to SAVVIS employees and have strict rules governing access to those areas.

3.15.8 Access to the High Security areas within the Data Center must be granted by the Facilities Team.

3.15.9 Contractors may not prop open exterior or interior doors unless approved to do so by the Facilities Team.

3.15.10 Contractors may not, under any circumstances, disable door sensors or alarms unless specifically directed to do so by a member of the Facilities Team with prior SAVVIS Security approval.

3.15.11 Alarmed doors are not to be used for egress unless approved by the Facilities Team.

3.16 SHIPPING AND RECEIVING

3.16.1 The Shipping & Receiving area is restricted and Contractors may not be in the area unless a member of the Facilities or Operations Teams is present in the area at all times.

3.16.2 All Contractors/Vendors must notify the Facilities Team of pending shipments. Any delivery attempt made without prior scheduling shall be rejected. Contractors must be on site to receive any large or heavy shipments.

3.16.3 The dock area is for unloading only – no parking is permitted. Contractor/Vendor

vehicles are to be parked in the locations specified by the Facilities Team.

3.16.4 If the dock area is used as a staging area for equipment and material to be brought into the Data Center, Contractors must clean up the area of their trash and debris prop to continuing their work inside the Data Center.

3.17 CUSTOMER CAGES

3.17.1 Access to the customer-occupied cages is strictly regulated. Access to a customer's cage can only be granted if a valid Siebel ticket has been opened detailing the specific scope of work to be performed inside the cage.

3.17.2 Only SAVVIS personnel are allowed to unlock and occupied cage for a Contractor to perform work.

3.17.3 Contractors inside a customer's cage are authorized only to perform only those tasks as detailed in the Siebel ticket.

3.17.4 Customer inquiries and requests directed to Contractors should be immediately referred to the Facilities Team.

3.17.5 An open customer-occupied cage in which Contractors are performing work must be secured (doors closed and locked) if left unattended for any length of time.

3.17.6 Contractors are not to remove anything from a customer's cage unless specifically directed to do so by the Facilities Team.

3.18 NODE AND MANAGED CAGES

3.18.1 Access to the NODE and Managed Cages inside the Data Center is severely restricted. Unauthorized entry in to the se areas is grounds for termination for SAVVIS employees. Contractors are not to enter these areas under any circumstances unless authorized to do so by the Facilities or Operations Team.

3.18.2 Any work to be done in the NODE or Managed Cages must have an approved Risk Assessment Form (RAF) in place before access can be granted.

3.18.3 Access into the Managed Cages and NODE must be approved by the Operations Manager or Facilities Manager.

3.18.4 All Contractors performing work in the Managed cages and NODE rooms must be escorted at all times by an Operations or Facilities employee.

3.19 PHOTOGRAPHY

3.19.1 SAVVIS prohibits taking any photographs of the exterior or interior of their Data Centers by Contractors or Vendors. Cameras inside a SAVVIS facility are strictly prohibited without Security authorization in advance.

3.20 POLICIES AND PROCEDURES

3.20.1 All personnel on the premises will follow the approved policies and procedures.

3.20.2 All activity within the data center is evaluated based on a level of risk associated with the activity. Planned and unplanned activities are classified from 1 to 5, 5 being the lowest level of risk. Planned activities are given a level of readiness (LOR) classification of 1 to

5 based on the task's effect on the redundancy of the critical systems. Each level has certain requirements that have to be met before work is performed. For more information see Facilities Level of Readiness, SV1-FAC-FPO-GEN-1115.

3.20.3 The five classification of risk are as follows:

3.20.3.1 LOR 1 - Life/Safety

3.20.3.2 LOR 2 - Critical – has or has the potential to interrupt IT load. Loss of N.

3.20.3.3 LOR 3 - Serious – no further backup systems are available. Loss of N+1. Also includes "hot work".

3.20.3.4 LOR 4 - Significant – Critical backup systems are available. N+1 intact.

3.20.3.5 LOR 5 - Advisory

3.20.4 Level 3, and above, tasks require two people, one to read the step and one to perform the work.

3.20.5 The Project Manager must be on site while level 3, and above, work is being performed.

3.20.6 "Hot work" is defined as all work on or around 100 volts to ground. All work on energized and de-energized electrical systems shall be done in strict accordance with OSHA 1910.333 and NFPA 70E.

3.21 ELECTRICAL INSTALLATION STANDARDS

3.21.1 "Hot Work" is defined as all work on or around 100 volts to ground. All work on energized and de-energized electrical systems shall be done in strict accordance with OSHA 1910.333 and NFPA 70E.

3.21.2 No work shall be done on any energized high voltage electrical components. All high voltage equipment must be de-energized and locked out.

3.21.3 Non-metallic fish tapes will be used for all electrical work.

3.21.4 All electrical circuits must be dedicated home runs with no splices or intermediate plugs or connections.

3.21.5 All electrical circuits in the data center will terminate in a female twist lock receptacle unless the circuit is hardwired directly to the hardware.

3.21.6 Power for rack or cabinet mounted equipment must be dedicated to that rack or cabinet.

3.21.7 Internally connecting power between adjacent racks or cabinets is not allowed.

3.21.8 Do not daisy chain power strips, i.e. one power strip cord plugged into a receptacle of another power strip to provide additional outlet receptacles. Each power strip should be a dedicated home run back to its own source of power.

3.21.9 Do not open any breaker unless positively identified by a circuit load verification test and directed to do so by an approved procedure.

3.22 LOCK-OUT/TAG-OUT PROCEDURES

3.22.1 Service technicians and mechanics must provide their own organizations procedures, equipment, locks and tags, and each tag must be filled out properly and legibly.

3.22.2 Lock-out/Tag-out of any device supporting the Data Center must be approved in advance by the facilities manager, witnessed, and approved by the Project Manager.

3.22.3 Any person working near or on de-energized equipment shall place their lock on the Lockout device.

3.22.4 Notify the Project Manager before unlocking any tagged out piece of equipment. Log all actions in the permanent TAG OUT LOG located in the NOC.

3.22.5 Do not remove or apply power to any piece of equipment without first informing and receiving clearance from Project Manager.

3.23 WELDING AND CUTTING PERMITS

3.23.1 You must acquire a Welding Permit or a Cutting Permit for any temporary operation involving open flames or which produces heat and/or sparks.

3.23.2 The Project Manager must fill out the Permit.

3.23.3 Be sure to adhere strictly to the Precautions Checklist contained on the Permit.

3.23.4 You must implement an approved means of ventilating smoke from the area (e.g.: HEPA filtration or exhaust outside the Data Center).

3.23.5 Notify the Project Manager upon completion of the work.

3.24 MECHANICAL WORK

3.24.1 The vendor's Supervising Technician/Mechanic must be a qualified Foreman or Journeyman with previous experience within the Data Center

3.24.2 Free liquids are not allowed in the raised floor areas. All liquids in these areas must have positive control.

3.25 DELIVERIES AND SHIPMENTS

3.25.1 All vendors must notify the Project Manager of pending shipments. Any delivery attempt made without prior scheduling shall be rejected. .

3.25.2 The vendor must be on site to receive any large or heavy shipments.

3.26 VACUUMS

3.26.1 To limit the amount of airborne particles, all vacuums used in the data center will have a HEPA discharge filter capable of limiting discharged particles to 0.3 microns.

Data Center Work Rules

Personal Accountability

Failure to know or comply with the Data Center Work Rules Policy, SV1-FAC-FPO-MGT-1427, is grounds for immediate removal from the site, perhaps permanently. All people allowed access to critical areas must review these Work Rules and demonstrate their knowledge of the Rules most applicable to their activity on site at least every twelve months.

It is vitally important that you understand the severe negative impact your actions can have on this site as a result of working inappropriately. These rules and guidelines have been developed to clarify our quality of expectations and to reduce the chance of mistakes and unintended events. Failure to comply with any procedure will result in your immediate removal from the site, may result in permanent loss of your access to the facility, and possible loss of business for you or your company.

I have been given a copy of the Savvis Data Center Work Rules for Construction and Maintenance Contractors and have read them. I have had an opportunity to ask clarifying questions about the rules, their reasons, and their intent. I agree to follow this policy and, to the best of my ability, I will make every effort to avoid accidents and mistakes, which will result in downtime.

Company _____

Name [print] _____

Signature _____ Date _____

Accepted by Savvis _____ Date _____