Section 01 Document Information	Centeris Data Centers - Security Procedure				
Creation Date:	12/1/2016	Revision Date:	2/28/2018	Effective Date:	2/28/2018

Section 02 Site Information	Site Information		
	Centeris Data Center	Document Number:	SP 1-16
	The Centeris Data Center exterior and interior premises are monitored 24x7 by a CCTV system and a motion activated digital video recording. Access to the interior is controlled using security issued access badges and badge readers. Interior access is granted only to areas of activity. Sensitive areas are controlled by a combination of access badge readers and fingerprint biometric readers. All access control is regulated and monitored by onsite security officer 24x7.		

Section 03 Details	Details

3.1 Purpose and Scope

- This procedure describes the physical security requirements and the authorization process by which personnel may obtain access to the Centeris Data Center.
- Compliance with this procedure is required for all personnel who work in or visit the data center.
- This procedure applies to all customers, visitors, staff and vendors of Centeris Data Center.

Section 04 Security Procedure	Physical Security/ Access Control

4.1 Exterior Security

- Access to the Data Centers exterior infrastructure is restricted to authorized personnel only.
- Access to the site is controlled by automated security gates requiring badge access or security staff permission for entry. Tailgating through the gates is not tolerated, each vehicle must identify themselves using the security call box before entering the site or scan their access badge at the front gate badge reader.
- All on site customers, visitors and contractors must check in at the security office to verify their identities using valid, government issued, identification. All individuals on site will be entered in to the visitor log software by security staff.

4.2 Server Cabinets

- Server cabinets and/or cages shall be maintained secured at all time.
- Access to server cabinets is restricted to authorized personnel only.

4.3 Man Traps

- The Centeris Data Center primary access corridor is equipped with an access controlled man trap. Two additional man traps are located in both the 1st and 2nd floor loading dock areas as major points of access.

4.4 Badging

- The access system is badge in and badge out. Each person must badge at each badge reader, at every point of entry or exit with a badge reader present.

4.5 Anti-pass-back

- The anti-passback system, monitors the badging activities of all individuals on site for violations of the badging procedure.
- Anti-passback is used in the data center hall and Main Distribution Frame (MDF) room.
- Violators will be placed in lockout status and will not be able to access any other location with the exception of the doors leading to the security office until the issue is resolved by security staff.

4.6 Keys and Badges

- All temporary access badges require an exchange of valid government identification as collateral for the badge to be issued. These identification cards are maintained secured by security personnel for the duration that they are on the premises.
- Assigned badges are not to be loaned out for any reason and must be worn visibly at all times while on site.
- All physical site keys require identification cards as collateral as well as a signature of the individual requesting the key. These keys are to never leave the site without prior authorization.
- All physical site keys assigned to personnel and will remain on person both on and off duty will require data center management authorization and will only be used by authorized personnel.

Section 05
Authorization Procedure

Provisioning Process for Authorization

5.1 Authorization

- Benaroya/ Centeris employees who require permanent access must be authorized by their supervisor.
- Centeris contracted personnel who require permanent access must be authorized by Data Center Manager and contractor management in writing.
- Customer personnel who require permanent access must be authorized by their management.
- Customer contracted personnel who require permanent access for the purpose of working on customer's co-located systems must obtain authorization from customer's management appointed authority prior to accessing the facility.
- Physical access to the facility shall not be granted on an "emergency" basis to individuals who have not been authorized to work in critical areas.
- Access must be renewed annually to maintain approved status.

5.2 Obtaining Authorization

- Authorized personnel must read and agree to the Security Policy and Procedures documents. Additionally, for work in critical areas, authorized personnel must read and sign the Centeris Data Center Critical Facilities Work Rules.
- Centeris Data Center Management must approve all access requests. Access requests must be submitted to Centeris Data Center management by an authorized manager via email to Centeris-SECURITY@centeris.com and will include:
    - Vendor name, purpose of visit, dates/times access is needed, requestor name and digitally signed by Customer's management.
- Managers of contracted service and maintenance personnel shall notify the Centeris Data Center management of employee terminations or changes in job assignment.
- For the purpose of the authorization procedure the following are Centeris mangers with the ability to grant authorization:
    - Permanent Badges;
        - VP of Operations, Data Center Manager
    - Temporary and Contractor Badges;
        - VP of Operations, Data Center Manager
        - Critical Facilities Manager, and Security Supervisor.
- All access badges will remain secured on site within the Centeris Security Office at all times. Exceptions are staff designated as emergency responders.
- Centeris Security Office will maintain all records for temporary access request.

Section 06

Vendor Protocol

Visitors, Contractors, and Customers

6.1 Customers, Contractors, and Subcontractors

- Maintenance visits by contractors and subcontractors who have not completed the "Authorization Process" must be scheduled in advance by their company management and approved by Centeris Data Center management.
- Emergency service visits by clients or their contractors who have not completed the "Authorization Process" may be authorized by contacting Centeris Security Office by email or by phone at 253-200-5053 or Centeris-SECURITY@centeris.com. The security office will pursue proper management approval. Service person will be escorted at all times. Under no circumstances a person that has not completed the "Authorization Process" will be allowed access to the Data Center unless Data Center management and security office received a confirmation from a Client's authorized manager.
- Upon signing the Critical Facilities Work Rules, customers or their contractors will be issued a access badge and may be escorted and/or under surveillance for the duration of their time on site.
- New staff within the customer's organization or client contractors who regularly require access in order to service equipment will be granted permanent badges in accordance with the "Authorization Process" which is detailed in the section above.
- Client contractors or representatives who have not completed the authorization process will be issued an "Escort Required" badge and must be escorted by either the customer who requested the service. Or when available a Centeris security officer or critical facilities personnel may perform this escort.
- All customers, contractors and subcontractors will use their government issued identification to receive a Centeris access badge.
- All customer, contractors and visitors must check in and out with Centeris Security Office security staff when coming and going from Centeris Data Center Property.
- All identification will be returned once the Centeris Security Office receives the issued access badge.
- All badges, unless designated emergency responder, must be returned to security at the end of each day, even if the individual will be returning the following day.

6.2 Visitors

- Any visitor entering the facility **must exchange** their valid government ID for an access badge for tracking purposes. Some situations may require escort. Example below but not limited to;
    - Visitors to onsite staff.
    - A tour group.
    - All minors will be issued escort only passes and must be accompanied by an authorized escort at all times.
- Visitor access badges are required to be returned to the Centeris Security Office at the end of each day even if the visitor will be returning the following day.

6.3 Emergency Responders

- Any staff designated to assist on site in the event of an emergency. This includes but not limited to, the assisting of other emergency responders such as the police, EMS, or fire department.

6.4 Lost/Stolen/Forgotten Access Badges

- If your access badge is lost or stolen, you are required to report the loss immediately to Centeris security at 253-200-5053 or Centeris-SECURITY@centeris.com. Centeris security may issue you a temporary badge until a replacement can be made for you.
- If you forgot your access badge and require access to the facility Centeris security will issue a temporary access badge for you to use while on site.

Section 07
Additional Rules

Additional Site Rules

7.1 Non-Disclosure

- As a condition of obtaining access to the facility, all staff, and third parties shall agree not to disclose any information they may obtain about the facility except to those who are required to have said information for conducting legitimate data center business.

7.2 Weapons

- No weapons will be allowed on site for any reason. This includes switchblades, stiletto, butterfly knives, brass knuckles and any knife with a blade longer than 4 inches.
- Violation of this policy will lead to immediate ejection from the site.

7.3 Photography/Videography

- Taking pictures and or video, including cell phones equipped with cameras, is prohibited without authorization from Data Center Manager.

7.4 Food, Drink, and Tobacco Products

- Food and drink are allowed only in designated areas. No food or drink are allowed in any of the server areas, the data center hall or near any electronic equipment.
- In accordance with Washington State law, no smoking will be allowed inside the facility, this includes vaporizers. Smoking will be allowed outside in designated smoking areas.

7.5 Related Procedures

- Critical Facilities Work Rules.
- Security Policy