SECURE ROOM CONTROLS

The following Secure Room Controls (“**Controls**”) must be implemented for Offshore Locations:

- Access methods and locations for vendors must be documented within the contractual language and engagement,
- Systems and data in scope must be clearly identified, as well as duration, type of access, and volume of data,
- The use of any offshore provider must be explicitly approved by Regions’ CISO prior to establishing any connectivity or access to Regions’ environments, network, Systems or data.

Physical Security Requirements – Any approved Offshore Locations utilized by Vendor and/or Vendor’s Approved Subcontractors and Affiliates (collectively, “**Vendor**”) are expected to provide a segregated and secure physical facility.

- Vendor must provide a dedicated secure room (the "**Regions Secure Room**") that is used for the sole purpose of performing Regions' contractual work. The Regions Secure Room must not be used to perform other contractual work unrelated to Regions or to process or access and data of Vendor’s other clients.
- If Regions’ data is to be hosted by Vendor, the servers must be physically separated and secured within a data center and approved by the Regions’ CISO in writing.
- Networking devices used to access Regions’ data must be physically separated and secured within a data center approved in writing by the Regions’ CISO.
- Physical barriers must be built from the natural floor to the natural ceiling to prevent unauthorized physical access. Dropped ceilings must be examined to ensure that separating walls continue to the true ceiling. Raised floors must be examined to ensure that separating walls continue to the true floor.
- All glass partitions must be treated to prevent any unauthorized view into the Regions Secure Room.
- In any area where glass is used, the Regions Secure Room must be partitioned off with glass break sensors installed.
- All doors must be locked, alarmed to prevent being left open, and electronic logs maintained for all entry and exit points.
- The Regions Secure Room access must be uniquely assigned to individuals and limited to those individuals who have a legitimate business justification.
- Physical access to the Regions Secure Room must be restricted by card access and biometric readers.
- Approved Personnel who access the Regions Secure Room must “badge in” and “badge out” every time they enter or exit the space. Piggybacking in behind another employee or contractor will not be allowed.
- Identification must be worn by approved Personnel while in the Regions Secure Room. Any approved Personnel not wearing identification will not be allowed into the Regions Secure Room.
- The use of Closed-Circuit Television (“**CCTV**”) must be deployed throughout the restricted areas of Vendor’s facility and must be placed in a position that allows for an individual to be clearly identified.
- CCTVs must cover the following sensitive areas:
  - All doors leading to and from Regions Secure Room;
  - Any document handling areas (i.e. printers, faxes, cabinets, desks conference tables, etc.);
  - Any communication areas such as phones (excluding phones connected to auto dialer systems);
  - All workstations within the Regions Secure Room;
  - Related conference and meeting rooms; and

  - Physically segmented networking environments.
- Monitor images and keystrokes must not be visible on the CCTV recordings.
- CCTV recordings must be proactively monitored and retained for future review for a minimum of ninety (90) days (the "**Review Period**"). Additionally, Regions requires secure storage and network connectivity for Regions owned DVR equipment for monitoring CCTV tapes and cameras. During the Review Period, the CCTV footage must be available to Regions upon demand.
- Unless specifically authorized in writing by Regions' CISO, the Regions Secure Room should be completely paperless. Where paper documents are permitted, the following apply:
  - Documents must not be taken into or out of the Regions Secure Room.
  - A clean workspace must be enforced to reduce the risk of unauthorized access to or the loss of information when areas are unattended.
  - All documents must be stored in locked cabinets when not in use.
  - All documents must be disposed of via secured document disposal bins or cross-cut shred within the Regions Secure Room.
- Only clear bags or purses will be permitted within the Regions Secure Room.
- Personal electronics with any photographic or recording capabilities must not be allowed within the Regions Secure Room.
- For Vendor call centers, phones other than those connected to the call dialer is prohibited.
- Vendor's phones are prohibited at the workstations; however, a limited number of phones may be permitted within the broader work environment if required for business related purposes.
- All requests for land-line phones within the Regions Secure Room must adhere to the following requirements:
  - Phones must be limited to for business use only.
  - Calls are subject to being monitored and recorded at the discretion of Regions. All phone recordings will be stored at Regions.
  - If call recording is not possible, phones must be restricted and only allowed to call an approved list of numbers.
  - For emergency calls from the outside, there must be a designated phone located at the managers' desk or in a general location within the Regions Secure Room (not at an agent's desk). This phone is only to be used for emergencies.

Logical Security Requirements - Vendor is expected to provide a secure logical environment for accessing Regions' environments, network, Systems, and data and for and implementing these controls at a minimum. Regions' data must not be processed or accessed on the same logical network or environment of Vendor's other clients.

- Connectivity to devices such as printers, scanners, faxes and phones must be disabled unless the device is physically and logically restricted to the same dedicated Regions Secure Room and solely for approved Regions contractual work.

- Logical and physical access rights must be revoked as soon as possible but not exceeding twenty-four (24) hours of an individual transferring to another project outside of Regions or voluntarily / involuntarily resigning from their employment.
- Vendor must utilize Regions' Secure Vendor Access (SVA) Portal and Regions' Virtual Desktop Infrastructure (VDIs) for remote access to the Regions network.
- The network remote access method for connecting to Regions must be reviewed and approved by Regions Cyber Infrastructure and Information Security teams, as may be identified by Regions.
- If Vendor is performing any of these functions then Vendor must have a private dedicated network connection to Regions that is used as the primary connection between Vendor and Regions' data center:
  - Provide direct support services to Regions customers;
  - Require real time access to Regions hosted applications; or
  - Require connectivity to Regions voice infrastructure.

- Availability and performance of the connection must be monitored by the party hosting the connection. On Demand Reporting must be available to Regions. Any interruptions of the connection or failure to meet availability or performance requirements must be reported to the Regions Network Operations Center in a timely manner.
- IP address restrictions must limit ingress and egress to known and business justifiable IP addresses necessary to perform the contractual work for Regions.
- Vendor servers and workstations facilitating connectivity must be fully patched and adhere to the following SLAs:
    - Operating System ("**OS**") and application patches: OS patches and application patches are applied within thirty (30) days of their release.
    - Any patches designated as emergency patches must be applied within seven (7) days of release.
- Remote workers are required to utilize multi-factor authentication to access Regions network.
- Connectivity to Regions must be encrypted using NIST-approved, current cyphers.
- Vendor Personnel accessing the Secured Room must successfully complete Regions' Information Security annual mandatory training.
- As permitted by local laws, Vendor Personnel must complete background checks to include criminal, employment, global database, and identity before they are allowed to work on any Regions engagements.
- Additional Regions Secure Room controls / requirements as contractually required.

Workstation Security Controls for the Regions Secure Room:

- Applications available via the desktop must be pre-approved by the Regions' CISO in writing.
- Laptops are prohibited in the Regions Secure Room.
- Wherever technically feasible, any Vendor server, network device, mainframe, internal application, or remote access facility that is in scope must utilize the following Regions Log-On Banner language to clearly communicate access rights to authorized individuals:
    - "Only authorized users may use this system ONLY for legitimate Regions business purposes. Information displayed, accessed, or processed on this system is to be treated as strictly confidential. There is no expectation of privacy in connection with your activities, the information handled, sent, or stored on this network. By accessing this system you accept that your actions may be monitored and/or recorded. Information gathered may be used to pursue any and all remedied available by law, including termination of employment or providing evidence of such monitoring to law enforcement officials."
- Deployment of Antivirus / Endpoint Detection & Response: Vendor must have the proper protections in place to monitor, detect, and protect OS from malware, threats, and anomalous behavior.
- Electronic Portable Media / DLP Endpoint: All electronic removable media / portable media should be physically removed or logically disabled (USB, memory cards, disk/CD/DVD drives, portable storage drives, etc.) and read / write functions must be restricted. Monitor and restrict sensitive data in motion via the network and prevent USB or removable media storage device usage.
- Web Content Filtering: Internet access is restricted to only approved destinations. Access to cloud storage sites, file uploads, chat, instant messaging services, and public webmail must be restricted.
- Secure Network Connection: System must be connected to a segregated, secured network only. A private dedicated network connection is required if Vendor meets certain requirements as stated herein.
- Latest, Regions Information Security approved OS: OS must be vetted by Regions Information Security and hardened according to CIS Benchmarks to ensure sufficient security configurations have been applied.
- Disable SMB File Sharing Access: SMB file sharing access must be disabled either using Group Policy or system policy to prevent lateral movement of potentially sensitive data.
- Disable Wifi, Bluetooth, and NFC Services: Wifi, Bluetooth, and NFC or any other wireless services must be disabled to prevent wireless file transfers.

- No administrative rights for user on desktop: Users must not be granted administrative rights to their profile or system to prevent unauthorized privilege escalation and ability to circumvent controls.
- Disable Printing Services: The ability to print must be restricted to prevent the unauthorized distribution of sensitive data.
- Disable Command Prompt, PowerShell, Notepad, MS Paint, Snipping Tool: OS built-in tools that could allow execution of malicious/unauthorized commands and/or perform data exfiltration functions must be disabled.
- Clear Screen/Clean Desk: Session timeout/lockout of no greater than fifteen (15) minutes must be enforced on workstations. Screens must not be visible from outside of the Regions Secure Room (e.g., Vendor can use screen privacy filters or angle screens away from windows, etc.) to prevent the unintended exposure of sensitive information. Desks should be clear from writing instruments and paper (the use of small white boards with dry erase markers are allowed provided they are wiped clean after each shift). Mobile phones and unapproved electronics are prohibited at workstations.

Monitoring: Upon Regions' request, Regions, or a Regions' vendor, will be allowed to physically audit Vendor's compliance with these Controls by observing Vendor's secure room operations through external viewing, either "through the glass" or through CCTV. In addition, annually Vendor must attest and provide evidence of compliance with these Controls that is acceptable to Regions CISO.