MINIMUM CYBERSECURITY REQUIREMENTS

Minimum Information Security/Cybersecurity Requirements	
	Administrative Control Requirements
A1	Vendor must have a documented Information Security Program based on Industry Standards utilizing a risk-based approach to ensure the security of Information Assets.
A2	Vendor's Information Security Program must describe organizational roles and responsibilities, including a chief information security officer (or comparable role).
A3	Vendor must implement reasonable risk assessment processes to identify weaknesses in its Information Security framework and remediate weaknesses in accordance with Industry Standards.
A4	Vendor's Information Security Program must be designed with reasonable administrative, technical (logical), and physical (including cameras, visitor logs, and badges where appropriate) safeguards.
A5	Vendor's Information Security Program must be reviewed at least annually or whenever there is a material change or an Information Security Event.
A6	Vendor's Personnel must be qualified and trained to address relevant cybersecurity risks in their role.
A7	Vendor must deliver, at least annually, cybersecurity awareness training for employees and, where applicable, contractors, appropriate and relevant to providing Deliverables and / or who have access to Regions' Information Assets.
A8	Vendor must perform background checks for employees and contractors which comply with applicable laws and are consistent with the risk assessment and access privileges required by the Personnel prior to employment and/or access to Regions' Information Assets.
A9	Vendor must conduct an appropriate security/risk assessment on all Systems, software, and devices, including new hardware/software, before they are used to Process Regions' Information Assets.
A10	Vendor must utilize "least privilege", "need to know", and "segregation of duties" access principles in their policies and procedures for Protected Information. It must be applicable to all Processing of Protected Information, whether in electronic, tangible, or other format or medium.
A11	Vendor must perform regular and periodic entitlement reviews to ensure adherence with defined access control policies and procedures as stated herein.
A12	Vendor must inventory, classify, and manage Information Assets according to Industry Standards.
A13	Vendor's information disposal/retention policies must meet the terms of the Contract and be designed and implemented appropriately based on data classification level, laws, and Industry Standards.
A14	Vendor must implement policies and procedures to maintain adequate vulnerability management practices which conform to Industry Standards.
A15	Vendor must have a documented Information Security Event Response Plan reasonably designed to detect, manage (including appropriate mitigation), and resolve Information Security Events.
A16	Vendor must implement and maintain a reasonable and documented cyber resiliency/BCP/DR plan sufficient to meet service level and data protection Requirements stated in this Exhibit and the Contract.
A17	Vendor shall comply with Industry Standards and all applicable laws and regulations for record retention/disposal requirements and, subject to legal retention requirements, shall not store or maintain any Regions Information Assets for more than one (1) year following termination of the Contract, unless specifically approved in writing by Regions. In all other instances, Vendor shall not destroy Regions Information Assets without Regions' prior written approval.
	Physical Control Requirements
P1	Regions Information Assets (excluding mobile devices secured in accordance with the Requirements) must not be physically removed from Vendor's premises without written authorization by Regions.
	Technical Control Requirements
T1	Vendor must implement Multi-Factor Authentication ("**MFA**") and other controls, as appropriate, for incoming remote connections to Systems or networks containing or Processing Protected Information, and for all system administration activities (privileged access).
T2	Vendor's access, identification, and authentication controls must conform to Industry Standards.

T3	Vendor's user accounts (including service accounts) with privileged access must: (i) align with Industry Standards; (ii) be secured appropriately; and (iii) be routinely monitored.
T4	Vendor must implement access and security controls for Regions Information Assets based on the classification of such assets and information and substantially consistent with Industry Standards.
T5	Vendor must implement access and security controls to meet regulatory requirements applicable for Information Assets and which may exceed the Requirements.
T6	Vendor must implement System hardening and continuous monitoring aligned to Industry Standards.
T7	Vendor must apply current, Industry Standard encryption to all Protected Information both at rest and in transit and shall also encrypt Systems and endpoint devices (including mobile and remote access devices) which Process Protected Information.
T8	Vendor shall not install or use any unlicensed and/or software not approved by Regions on any Regions Information Asset or on Vendor Information Assets used to Process Protected Information.
T9	Vendor must install and monitor anti-malware and antivirus software on all Vendor Systems and devices with access to Protected Information.
T10	Vendor Systems and endpoint/mobile devices must employ up-to-date software with patches and security updates applied promptly in accordance with Industry Standards.
T11	Vendor must configure Systems and network devices to employ filtering to deny unauthorized inbound and outbound network traffic.
T12	Vendor must logically segment or segregate Protected Information from other systems on internal Systems and networks. Vendor shall also digitally and physically separate production and non-production environments and shall not use Protected Information in a non-production environment.
T13	Vendor must secure or disable unattended network ports and implement appropriate security on wireless networks and access points to prevent unauthorized access and connections.
T14	Vendor's network and infrastructure must be reasonably designed to protect and defend against malicious activity, including, without limitation, denial-of-service and ransomware attacks.
T15	Vendor must implement and monitor network-based intrusion detection / intrusion prevention systems that align to Industry Standards.
T16	Vendor must perform penetration and vulnerability testing at both the network and application layers of Information Assets Processing Protected Information in accordance with Industry Standards and patch/remediate in accordance with Industry Standards. Vendor agrees to provide testing results to Regions; provided that Vendor is not required to disclose confidential or proprietary information.
T17	Vendor may not connect any device to Regions' Systems without Regions' approval.
T18	Vendor must implement daily logging and monitoring of Systems which Process Protected Information consistent with Industry Standards and sufficient to meet the Requirements to detect and respond to Information Security Events and, where applicable, sufficient to reconstruct material financial transactions. Vendor agrees, where applicable, to provide copies of logs to Regions for SIEM ingestion.
T19	Vendor must follow practices designed to develop business applications in accordance with Industry Standard methodology, design, secure coding, and testing requirements.
T20	Vendor must implement routine and emergency change management controls requiring that changes are requested, authorized, tested, documented, approved, and periodically reviewed.
T21	Vendor must maintain a code development/implementation plan that identifies risks and establishes a back-out procedure, which plan must be reviewed and approved by Regions.
T22	Vendor must implement back-up/restoration policies and procedures sufficient to meet BCP/DR recovery objectives and service level requirements stated in this Exhibit and in the Contract. All Protected Information stored in back-up media must meet minimum Requirements and the terms of the Contract.
T23	If applicable, Vendor must comply with PCI standards when Processing payment card information and provide evidence of compliance to Regions at least annually and for as long as Vendor Processes PCI Data.