The HITRUST MyCSF offers organizations numerous benefits for enhanced assessment and remediation capabilities, while also serving as a software as a service (SaaS), that continually updates and maintains the content and application environment for the HITRUST Common Security Framework (CSF).

HITRUST recognizes the sensitivity and concerns surrounding the third party hosting of an organization’s sensitive data. This document provides information on the safeguards, practices and technologies implemented by HITRUST, to protect the MyCSF environment.

Information Protection Program
HITRUST leverages the CSF and CSF Assurance Program, to provide a robust information protection program. Designed from the “ground up,” the program allows for the confidentiality, integrity and availability of the sensitive risk information contained in MyCSF.

Endpoint Protection
Servers and network components are hardened prior to, “go live.” By default, all ports are closed so that each new server is unable to communicate until specific rules have been identified, defined and implemented. All servers are configured with anti-virus/anti-malware, host-based firewalls and intrusion detection systems. New software versions, patches, heuristics, signatures and rule sets are also evaluated and implemented based on risk to the information and impact to the user.

Configuration Management
Development and test environments are logically separated from production and all changes by the application vendor and host provider are vetted and approved prior to implementation in the production environment.

Vulnerability Management
Antivirus/anti-malware and network/host-based intrusion detection systems are routinely updated to ensure the most robust protection against known and zero-day threats. Internal and external vulnerability scans are conducted no less than monthly, and all vulnerabilities are addressed by either the host provider, application vendor or by HITRUST. This is done through patching, configuration changes, intrusion detection and by monitoring use cases, to ensure the most robust protection of sensitive data from cyber threats.

Network Protection
Network-based application-level firewalls and intrusion detection systems are used to protect the network perimeter. Every MyCSF server is also protected through hypervisor-based firewalls, which provide granular protection for each security zone. Additional services include, dynamic DDOS protection and IP reputation filtering.

Transmission Protection
All transmissions to and from MyCSF are conducted through SSL VPNs. Internal communications between the application and database are similarly protected with, “transparent database encryption,” in which data is only unencrypted in memory and unencrypted data is never written to the disk. MyCSF also includes a native secure email capability, to support user workflow management.

Password Management
HITRUST’s service ensures passwords meet all CSF complexity, aging and other password-related requirements, as well as include a two-factor, end-user authentication.
Access Control
User access is controlled through HITRUST’s service and all administrator access is provided through two-factor authentication. Users are provided granular access based on defined roles and are assigned to groups where appropriate. The application also provides decentralized security administration and enforces segregation of duties.

Audit Logging and Monitoring
All server, database and MyCSF application access and activity is logged and correlated by a security information and event management system. Specialized security engineers, proactively monitor live security data points 24/7, in order to react quickly to potential problems.

Education, Training and Awareness
All HITRUST, host provider and application vendor personnel, receive annual security training. HITRUST personnel are also kept aware of the latest security issues affecting MyCSF, via periodic email alerts and weekly staff calls.

Third Party Assurance
MyCSF is implemented in a CSF Certified cloud-hosting environment that meets or exceeds regulatory compliance requirements. Vendors are similarly vetted to ensure they meet or exceed industry standards for software development and implementation.

Incident Management
The host provides robust incident management support for MyCSF, and HITRUST leverages its cybersecurity command and control (C3) capability, to ensure constant awareness of ongoing threats and the latest attack responses.

Business Continuity and Disaster Recovery
MyCSF is hosted on high-availability infrastructure, including DNS failover and load balancing, to help ensure continuity of service.

Risk Management
By vetting host and application providers against the CSF, HITRUST ensures that risks are constantly monitored and addressed.

Physical and Environmental Security
HITRUST’s CSF-compliant data center, provides industry best practices for physical and environmental security. This includes, employee and contractor background checks, two-factor authentication for physical entry throughout the host facility, 24/7 visual monitoring of sensitive workspaces, robust water and fire detection, alerting and/or suppression.

Data Protection and Privacy
Adherence to CSF control requirements provides MyCSF users with the utmost assurance that their sensitive data is protected, according to relevant standards and industry best practices.

For more information and resources, visit the MyCSF web page. Pricing for MyCSF is available by contacting HITRUST at 469-269-1110 or sales@hitrustalliance.net, or by viewing the pricing sheet.