# INFORMATION SECURITY

The DIFZ Team brings experience working with a wide variety of Federal Agencies to implement their information security programs. The examples below from DIFZ and teaming partner PPD demonstrate our experience and extensive IT security expertise and resources that we have deployed in Federal contracts. We will implement NCI’s security program in compliance with HSPD and FISMA.

**Integrated Security Architecture.** DIFZ has provided IT security-related research and engineering support to the Centers for Medicare and Medicaid Services (CMS) Information Security and Privacy Groups’ (ISPG) DevSecOps (DSO) Team in compliance with HSPD and FISMA since 2016. As part of ISPG’s DSO Support Team, DIFZ plays a key role in the development of high-value DevSecOps-related solutions that ensure security is “built-in” throughout all phases of each CMS system’s life cycle. Supporting the CMS CISO’s development of DevSecOps approach DIFZ successfully design and demonstrates ISPG’s DevSecOps automation solutions which have assisted with the modernization of the CMS ATO process through automated security compliance testing and documentation through integration of security testing tools into existing CI/CD pipelines. Through automation, the DIFZ DSO solutions team help promote continuous code validation, change, and configuration management.

Development Teams and ISPG Assessors analyze security data to generate accurate documentation at each Sprint/Release and support faster ATO decisions. The DIFZ Team integrates security baseline hardening and compliance testing into the CI/CD pipeline for cloud applications through development and integration of Chef InSpec Profiles, an open-source framework for testing and auditing applications and infrastructure, into those existing DevSecOps pipelines. Developers maintain agile code delivery, while satisfying compliance requirements and improving internal Security Impact Assessments (SIA). The DIFZ Team also supports development of data protection solutions at rest and in transition that include cost-effective strategies for encryption, secrets management and access control, leveraging existing investments at CMS.

**Security Technology Infrastructure.** Our teaming partner PPD has experience providing secure data center services; their two primary data centers (in Durham, NC and Austin, TX) house the infrastructure that hosts applications used to support the clinical trial process and corporate support functions. These data centers are built to specifications to ensure physical security, hardened to prevent intrusion, and supported by back-up power sources. Their production data center is compliant with HIPAA, Federal Information Security Management Act (FISMA) (High), FedRAMP, ISO 27001, and Payment Card Industry Data Security Standard (PCI DSS) standards. Standardized processes ensure data is backed up. All back-ups are replicated between the two data centers. Only authorized IT staff or facilities staff have data center access. Visitors must be escorted by authorized staff.

**IT Security Plan.** DIFZ Team recognizes that secure physical facilities integrated with strong IT infrastructure, data, and document storage are keys to sensitive data protection, project communications, cost control, and an enhanced user experience. Our strategic investment in technology creates the backbone for communications, management, processing, and storage of data. Robust facilities and a computing infrastructure built on best practices and industry-standard hardware and software result in secure and efficient administration of communications, data collection, data management, and storage requirements for hundreds of studies.

Information security risk assessments are completed on external vendors to ensure they have the appropriate controls in place. Information security risk assessments are completed on systems that include relevant responsibilities for review, scope, frequency, risk mitigations actions and approval. SOP IT-04 (Computer Room and Data Security) includes the high-level requirements and process for data backup and recovery. Additionally, WPDs detail the process by specific OS. Test restores are required at least semi-annually for each type of back-up application. Back-up and disaster recovery procedures follow the Disaster Recovery Master Plan, SOP IT-05. Databases can be recovered based on the use of offline backup/recovery, online backup/recovery or logical back up/recovery techniques. Additionally, systems requiring 24x7x365 availability implement high-availability strategies.

**Security Environment.** DIFZ Team operates under standard policies and procedures that provide a framework for information security. We use best security practices as a basis for our information security program and a defense-in-depth strategy to assure confidentiality, integrity, and availability of our sponsors’ sensitive data. Their environment is composed of computers, operating systems, applications and services, networks, operations and monitoring equipment, and specialized hardware, along with the administrative and operations staff required to run and maintain the services. The data centers are also included as part of their security posture; all data center services and physical access have safeguards in place to deter from any malicious or accidental damage.

The DIFZ Team chose to adopt the ISO 27001 framework due to the global nature of our provided services, receiving ISO/IEC 27001:2013 certification in 2020 and recertification in 2021.

**IT Security Policies and Procedures.** The DIFZ Team operates under a standard set of policies, SOPs, Best Practices & Guidelines (BPGs) that provide a framework for our information security environment. The DIFZ Team can provide a full listing of these policies, SOPs, and BPGs during competitive range negotiation responses.