SCHEDULE E

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Data Recognition Corporation (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

   DRC ensures that our clients' data remain confidential and secure at all times. Our practices adhere to the federal Family Educational Rights and Privacy Act (FERPA) regulations for the security and confidentiality of student data, and our systems provide data privacy safeguards throughout every step of an assessment process. While FERPA provides a foundation for DRC's data privacy policy, we view these as a baseline set of requirements. We work with our clients to meet FERPA as well as state-specific requirements and policies for securing student data.

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

   Our practices adhere to the federal Family Educational Rights and Privacy Act (FERPA) regulations for the security and confidentiality of student data, and our systems provide data privacy safeguards throughout every step of an assessment process. While FERPA provides a foundation for DRC's data privacy policy, we view these as a baseline set of requirements. We work with our state clients to meet FERPA as well as state-specific requirements and policies for securing student data.

DRC does not sell data, personal data or otherwise, and DRC does not retain, use, collect or disclose it other than for the specific purpose of performing the services specified by our clients. The data DRC collects is owned by our clients and we will follow their direction on its use. If an individual makes a request for their data be removed from our systems, DRC will differ to our clients, the data owners, to verify the individual and their request. DRC will follow our client's direction on the removal of any personal information as long as that removal does not compromise the integrity of any required reporting or other services.

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

   DRC holds our supply partners to the same high standards we hold ourselves. Partner companies and vendors are only granted access to data that is necessary to fulfill their role on the project. Access is restricted and monitored to ensure data always remains secure. All vendors are fully vetted and carefully monitored for security measures and performance as a part of DRC's Vendor Management Program. Security practices are documented and embedded into DRC's ISO 9001:2015-certified processes that span the entire chain of custody of testing materials and data.

   To ensure we are complying with our vendor management and security standards, DRC has embedded security documentation within the DRC Quality Management System. All vendors are audited as part of DRC's Vendor Management Program. These ISO-certified quality practices are audited several times a year by DRC Internal Audit staff and a third-party assessor.

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

   All vendors are fully vetted and carefully monitored for security measures and performance as a part of DRC's Vendor Management Program. Security practices are documented and embedded into DRC's ISO 9001:2015-certified processes that span the entire chain of custody of testing materials and data.

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

   DRC has a documented Incident Response Standard. This standard is implemented by DRC's Incident Response Team, which is composed of various IT professionals throughout the organization.

   The Incident Response Standard provides guidelines for responding to and recovering from a security event. Responsibilities and procedures are fully documented for the Incident Response Team. These include procedures for:

- Monitoring, detecting, assessing, and classifying security events
- Response, escalation, recovery, and tracking
- Documentation, communication, and reporting
- Collection, protection and preservation of relevant system and application information, and other relevant evidence pertaining to the event for future forensic and applicable legal requirements
- Post-event review for process improvements for prevention, early detection and remediation

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

   DRC works will each client on their specific needs and requirements for the secure transfer of data to the client and/or their designee using industry-leading encryption methods.

   DRC establishes a data retention plan with each client that governs how long various types of data are retained and when the data should be deleted and/or destroyed.

   DRC will comply with destroying the active data on our systems.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

NAME OF CONTRACTOR: Data Recognition Corporation

BY: Jennifer Eastman **DATED:** 10 · 29 · 20

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

Vendor's DATA SECURITY AND PRIVACY PLAN is as follows:

The DRC INSIGHT portal provides tiered access for all district and school staff involved in the administration of the LAS Links assessments. These functions are controlled through **a variety of security levels to ensure a user only views or edits data for which the user is authorized.** Users must login with a pre-determined unique user ID and password to gain access to the system. The system automatically enables or disables access to specific functions based on the user's profile and permissions.

High-level administrator accounts control the permissions and level of access each sub-user will have. The portal is permissions-based, meaning that users with administrative rights need to select what role a sub-user has and assign permissions to that individual. This allows the flexibility for users to have the same roles but different permissions. The district can set up users with as much or as little permission as deemed necessary. A user's role and permission may be modified at any time.

To promote the security and confidentiality of student data, new users are prompted to review and agree to a security and confidentiality agreement upon logging into the system for the first time. The user agrees not to disclose any student information from the system to anyone other than a state, district, or school official as defined by the federal Family Educational Rights and Privacy Act (FERPA).

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at:
http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, Or, by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   DRC collects only the minimum amount of protected information necessary to associate assessments and assessment results to each individual student. Unless specified by the client, DRC will not collect any other demographic or identifiable information. DRC complies with all state and federal laws, rules and regulation pertaining to individual security and privacy rights for protected information.

2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

   DRC holds our supply partners to the same high standards we hold ourselves. Partner companies and vendors are only granted access to data that is necessary to fulfill their role on the project. Access is restricted and monitored to ensure data always remains secure. All vendors are fully vetted and carefully monitored for security measures and performance as a part of DRC's Vendor Management Program. Security practices are documented and embedded into DRC's ISO 9001:2015-certified processes that span the entire chain of custody of testing materials and data.

   To ensure we are complying with our vendor management and security standards, DRC has embedded security documentation within the DRC Quality Management System. All vendors are audited as part of DRC's Vendor Management Program. These ISO-certified quality practices are audited several times a year by DRC Internal Audit staff and a third-party assessor.

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   DRC will securely transfer data to ESBOCES, or a successor contractor at the ESBOCES's option and written discretion, in a format agreed to by the parties. DRC will comply with destroying the active data on our systems.

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

   Pursuant to its contractual obligations, the Contractor will work with the ESBOCES in processing challenges to the accuracy of student data in the custody of the Contractor.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

   All data are stored in secure data centers only in the United States. All student data are fully secured before, during, and after testing, including demographic information about the student, the student's answers to questions, and the scores the student receives. Access to student data is only granted to those DRC employees and client personnel who are directly working on data-related tasks associated with the assessments. Only client staff who are authorized are allowed to access data, and they must sign a confidentiality statement agreeing not to disclose student information to anyone other than an approved official.

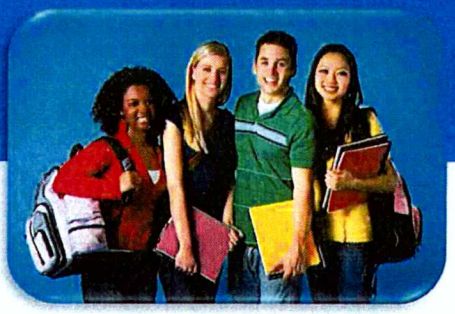
Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.

DRC's Data Privacy and Security Plan



DATA RECOGNITION
DRC
CORPORATION


DATA RECOGNITION
DRC
CORPORATION

Data Recognition Corporation's Data Privacy and Security Plan

Table of Contents

1. INTRODUCTION

Data Recognition Corporation (DRC) is an industry leader in successfully delivering high-stakes, large-scale assessments. DRC's current education product base, including numerous state-wide custom programs and assessment solutions, are developed in accordance with strict security standards and practices. **Our clients can be assured that all assessment materials, information technology, online systems, student responses, and data is handled and stored in a secure manner.**

DRC has security measures in place to both prevent and detect data breaches and other threats to our systems. This two-pronged approach continues to be very successful in securing and protecting our clients' data.

Ensuring security is critical to maintaining the technical quality, fairness, and integrity of any testing program. DRC is well-known within the educational assessment community for our unwavering commitment to meeting industry standards for quality and security. All assessment materials, information technology, online systems, and student responses and data are handled and stored in a secure manner, in compliance with many state departments of education needs and Federal laws and regulations.

DRC's security does not just involve the Information Technology Department, but rather is an enterprise-wide endeavor. We have policies and procedures in place to manage and protect information throughout every phase and in every component of a large-scale testing program, including applications and technology, facilities, processes, and people. With over 40 years of experience managing confidential client data, we have fine-tuned our security systems, disaster recovery processes, and data security procedures to consistently meet industry requirements.

DRC's Data and Information Management System

A summary of our security practice is shown in the following table.

Summary of DRC's Security Policies and Procedures

Security Component	Policies and Procedures
Facility and Personnel Security	• Mandatory employee key-card picture ID badges to enter and work in DRC facilities. • Secure access system logs all persons entering facilities, including all after-hours/weekend activity. • Mandatory visitor sign-in and temporary badges; all visitors accompanied by DRC employees. • Data centers meet industry standards and best practices for construction, climate control, fire suppression, redundant network infrastructure, power and cooling, and physical security. Facility are staffed with security guards 24 hours a day, 7 days a week. • Limited key-card and biometric access to data centers with all access logged. • Annual security and confidentiality training and employee-signed agreements.
Information Technology Security	• Full-time IT security administrators. • Security Team regularly assesses security policies and processes to ensure services and systems adherence to relevant security, availability, processing integrity, confidentiality and privacy requirements. • Third-party NIST 800-53 based FISMA audits, SSAE16 SOC 2 Type 1 audits, and ISO 27001 certifications as well as penetration testing are performed annually. • Full array of security technologies, including audit trails, firewalls, intrusion detection, intrusion protection, vulnerability scanning, anti-virus, source-code security, Secure Sockets Layer (SSL), and Security Information Event Management (SIEM) monitoring. • Data transferred using industry-leading encryption methods. • Strong passwords required for all employees to access any data. • Identity and Access Management (IAM) system restrict access to data and electronic files to only authorized personnel. • Data access restricted solely to personnel who need access to carry out responsibilities. • All confidential data are stored on systems and facilities maintained within DRC's networks, behind firewalls and only at locations in the United States. • Personal information is not sold and is retained, used, collected or disclosed only for the specific purpose of performing explicitly authorized and contracted services. • Maintain redundant backup copies, data replicas, and off-site storage of all data in secure facilities. • In-place disaster recovery plan for all systems and data.
Test Development and Psychometric Security	• Electronic item banking system (IDEAS) secured through password protection, user authentication, and SSL protocol. • All hard copies of item and form development materials physically secured. • Mandatory signed security agreements for all committee members. • Secure materials monitored at all times during committee meetings. • Proprietary data forensics system to systematically analyze data and ascertain integrity of data results.

Summary of DRC's Security Policies and Procedures

Security Component	Policies and Procedures
Online Test Security	• Password-protected, role-based access to administrative functions. • Secure student test access using a unique username and password (test ticket). • Encrypted data transfer. • Test content is decrypted and downloaded only when the student login is validated. • Device is secured during testing to prevent copying/printing and accessing other applications. • Test content is purged from device memory upon completion of test session. • If test is paused, the test content is removed from the screen; system times out after a defined period of inactivity.
Paper Test Security	• In-house production and printing of test materials. • Unique security code pre-printed on each secure document to unequivocally associate it with one record in a master database. • Barcode technology accurately tracks materials through all assessment phases. • All shipping vendors provide online tracing and tracking services. • Immediate secure materials check-in and processing.
Scanning, Scoring, and Reporting Security	• Student responses scored without inclusion of personally identifying information. • All scanning and scoring, including handscoring, conducted at fully secure facilities. • Mandatory reader (scorer) signed confidentiality agreements. • All data contained in secure databases. • Monitoring of distribution of hardcopy reports through online delivery tracking services. • Electronic results delivered through secure, password-protected report delivery system, with user-level access.

2. DRC'S SECURITY STANDARDS AND CERTIFICATIONS

DRC regularly reviews our security features, systems, and procedures to ensure compliance with all applicable federal laws including the Americans with Disabilities Act (ADA), the Every Student Succeeds Act (ESSA), the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), Sections 504 and 508 of the Rehabilitation Act, and Title I—Improving the Academic Achievement of the Disadvantaged.

DRC's online systems have all been designed to provide the level of security demanded by today's high-stakes assessment programs. With the advent of online testing, states are particularly concerned about how we protect student data and personally identifiable information (PII), as required by FERPA. To assure clients of our commitment to information security, **DRC's information security policies and procedures are based on the National Institute of Standards and Technology (NIST) criteria (NIST Standard 800-53)**. This is a nationally recognized standard with extensive requirements for information security practices.

To demonstrate that we meet the security expectations of our customers, **DRC holds ISO 27001:2013 certification**. Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), **ISO 27001 is the most internationally recognized information security standard in the world**. The ISO 27001:2013 standard specifies requirements for

establishing, implementing, maintaining, and continually improving information security management systems and includes requirements for the assessment and treatment of information security risks.

DRC processes hundreds of millions of secure transactions annually for departments of education, Federal and state government agencies, colleges and universities, and healthcare and financial institutions.

DRC is also a full-service research partner for the Federal Government. We are well known among Federal agencies as a low-risk, high-quality partner, as evidenced by the fact that clients such as the U.S. Department of Defense, U.S. Department of Veterans Affairs, Defense Health Agency, and the Internal Revenue Service trust us to complete some of their most important research programs and protect highly sensitive client data.

- For our work with the U.S. Department of Defense, DRC's Survey Services' systems are compliant with the NIST Risk Management Framework (RMF), and we manage our Information Systems under the NIST RMF policies and procedures. NIST RMF compliance encompasses a stringent set of security requirements in order to process and store Department of Defense data. DRC is one of only a few full-service survey research firms with this high-level of certification.
- DRC prints customer satisfaction surveys for the Internal Revenue Service (IRS). The data files for printing and mailing contain tax return information and personally identifiable information (PII). DRC undergoes annual security audits and has been approved by the IRS for meeting the stringent security requirements of this contract.
- DRC is also compliant with Health Insurance Portability and Accountability Act (HIPAA) security requirements for work with our healthcare clients, including numerous healthcare-related surveys for the U.S. Department of Veterans Affairs.

DRC's extensive security policies meets the most stringent security requirements for our state and Federal programs. Our industry-leading security credentials and standards are summarized below.

DRC's Security Standards and Certifications

- Adherence to federal FERPA regulations for the security and confidentiality of student data
- Adherence to NIST Standard 800-53, Rev 4
- Adherence to the ISO 27001:2013 information security system standards within our Document Services and Survey Services businesses
- Adherence to Statement on Standards for Attestation Engagements (SASE) No. 18 Service Organization Control (SOC) 2 Report requirements
- Compliance with NIST RMF for work with the U.S. Department of Defense
- Annual security audits for printing and distribution services contract with the Internal Revenue Service
- Compliance with HIPAA security requirements for contracts with healthcare clients

2.1. Annual Security Audits

DRC is committed to performing regular third-party audits to ensure our security processes are properly and consistently implemented and meet industry best practices. We currently receive third-party assessments from several independent organizations each year.

- To assure clients of our commitment to information security, the DRC INSIGHT online systems are annually audited against the NIST Standard 800-53. This is a nationally recognized standard for information security practices. DRC has engaged an independent, third-party information security firm to perform the annual audits of our DRC INSIGHT environment.
- DRC annually engages a third-party firm to conduct penetration tests on our network that supports the DRC INSIGHT system. These "attacks" attempt to gain unauthorized access to our network over a multiple-day period.
- DRC's ISO 27001:2013 certification also performs an annual third-party assessment which confirms DRC's services and systems adherence to relevant security, availability, processing integrity, confidentiality and privacy requirements. The ISO 27001 information security standard complements our existing quality management practices that are certified to the ISO 9001:2015 quality management standard. Blending our information security and quality standards strengthens DRC's business processes.

DRC's rigorous ISO 9001:2015 and ISO 27001:2013 certifications allow us to blend our information security and quality standards, strengthening DRC's business processes.

- In addition to the ISO 27001 and FISMA NIST 800-53 base audits, DRC performs an annual Statement on Standards for Attestation Engagements (SSAE) No. 18 Service Organization Control (SOC) 2 Report on the DRC INSIGHT systems. The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system.
- DRC also undergoes regular audits by some of our current clients, such as UnitedHealth Group, the Internal Revenue Service, and RBC Wealth Management.

DRC's compliance to national and international security standards, and the external validation requirements around them, allows clients to have confidence in their partnership with DRC.

2.2 Remediation

Audit findings are remediated with a focus on medicating risk to an acceptable level or eliminating risk by full remediation of the finding. Finding are assigned and appropriate subject matter experts (SME) and stakeholders perform a risk assessment and develop Plan of Action and Milestones (POAM) which includes a remediation plan, establish target dates and milestones. All open findings are tracked and reviewed regularly based on the risk assessment until they are closed.

2.3 Data Privacy and Use Policy

DRC ensures that our clients' data remain confidential and secure at all times. Our practices adhere to the federal Family Educational Rights and Privacy Act (FERPA) regulations for the security and confidentiality of student data, and our systems provide data privacy safeguards throughout every step of an assessment process. While FERPA provides a foundation for DRC's data privacy policy, we view these as a baseline set of requirements. We work with our state clients to meet FERPA as well as state-specific requirements and policies for securing student data.

All DRC staff members receive training on data security and confidentiality requirements, including annual Cyber Security Awareness training and assessment. In particular, DRC realizes the importance of keeping Personally Identifiable Information (PII) data secure at all times. We follow stringent procedures to protect PII data and frequently verify these procedures to confirm adherence.

All student data are fully secured before, during, and after testing, including demographic information about the student, the student's answers to questions, and the scores the student receives. Access to student data is only granted to those DRC employees and client personnel who are directly working on data-related tasks associated with the assessments. Only client staff who are authorized are allowed to access data, and they must sign a confidentiality statement agreeing not to disclose student information to anyone other than an approved official.

DRC does not sell data, personal data or otherwise, and DRC does not retain, use, collect or disclose it other than for the specific purpose of performing the services specified by our clients. The data DRC collects is owned by our clients and we will follow their direction on its use. If an individual makes a request for their data be removed from our systems, DRC will differ to our clients, the data owners, to verify the individual and their request. DRC will follow our client's direction on the removal of any personal information as long as that removal does not compromise the integrity of any required reporting or other services.

DRC does not share student data with third parties unless approved by the appropriate client authority. Likewise, we do not use student data for any purposes other than those required by the client. All data are stored in secure data centers in the United States. Product data are stored in a separate database instance and are not co-mingled with other client data. All data are captured and stored on a secure, protected server.

2.4 Least Privilege Data Access

DRC provides systems access to systems and data in accordance with the principle of least privilege. Individual data access rights start with limited access. If individuals do not have a business need for access, access is not granted. When access is authorized, accounts are assigned the minimum level of privilege necessary for the role.

These principles also extend into the client services. Client staff who have been assigned administration roles in the portal administration system have the ability to place others into specific roles, with privileges appropriate to them. The administration of the environment conforms to the role-based access needs of each client.

3. DRC'S CORPORATE SECURITY MEASURES

3.1. Information Technology, Facility, and Personnel Security

The security measures described in the figure below are in place at DRC.

DRC's Information Technology, Facility, and Personnel Security Controls

Information Security Program Management
• Full-time, experienced IT security administrator and Security Team, who oversee the implementation and operational aspects of technology security for the company. • Security Team enforces security policies and standards and performs ongoing mitigation of risk and vulnerability management.
Information Security Risk Management
• Full array of security technologies, including audit trails, firewalls, intrusion detection, intrusion protection, vulnerability scanning, anti-virus, source-code security, Secure Sockets Layer (SSL), and Security Information Event Management (SIEM) monitoring. • Manage hundreds of terabytes of client data; therefore, security is an inherent, inextricable, and indispensable component of our system. • Proactively identify areas of risk to ensure remediation.
Information Security Policies and Standards
• Stringent information security policies and standards are in place. • Policies are reviewed and updated on an annual basis. • Regular audits are performed to ensure compliance with policies and standards.
Information and Technology Compliance
• DRC's information security policies are based on, and annually audited against, the NIST criteria (NIST Standard 800-53). • DRC actively configures our systems and processes to comply with the ISO 27001 information security system standards. • DRC services and systems adhere to Statement on Standards for Attestation Engagements (SSAE) No. 18 Service Organization Control (SOC) 2 focusing on non-financial reporting controls related to security, availability, processing integrity, confidentiality, and privacy of a system. • DRC follows CIS Benchmark best practices for the secure system configuration. • Compliance with NIST RMF for work with the U.S. Department of Defense. • DRC undergoes annual security audits for current clients.
Business Continuity and Disaster Recovery
• Disaster Recovery Plan is in place to provide guidelines for when an unexpected or undesirable event occurs that disrupts the normal operations of the company. Copies of the plan are kept in a secure location on-site, at off-site locations, and with the emergency response coordinator. The plan is reviewed and updated annually or as needed. • Emergency response and business continuity strategies and procedures apply to all core operations at DRC. • Data backup process includes redundant backup copies, data replication, and off-site copies. • In-place disaster recovery plan for all systems and data. DRC uses a high-speed fiber ring for network redundancy and has a secondary data center in the case of a disaster.

DRC's Information Technology, Facility, and Personnel Security Controls

Security Awareness Training and Assessment
• DRC personnel are trained in security requirements, which include physical building access, employee confidentiality and behavior, data access, network and Internet access, and the safeguarding of client documents and products. • Security awareness materials are reviewed on an annual basis and annual Cyber Security Awareness training and assessment takes place. • DRC tracks and requires all employee complete the assessment annually. • Regular phishing exercises are performed and tracked throughout the year to maintain employee awareness to phishing attempts.
Identity and Access Management
• Data protection starts with a process that denies everyone access to data, and then specifically grants access to those authorized. DRC's identity and access management is controlled through Active Directory, whereby users are given the lowest level of access required to perform their jobs. • Any changes in system access follow our formal change management process. • Passwords—which must be strong, unique, complex, and changed regularly—are required for all personnel to access any data. Data and electronic files are accessible only to authorized personnel. • Access is regularly audited and immediately disabled whenever personnel leave DRC.
Security Incident Response and Forensics
• In the event of a security incident, DRC's Incident Response Team is trained to follow an organized approach to address and manage the situation. • The team is poised to handle the situation in a manner that limits damage and reduces recovery time by following our Incident Response Plan. • All security events are logged to a SIEM solution that provides the ability to retrieve data forensics should a security incident occur.
Information Security Monitoring
• Robust data loss prevention system that continuously scans and monitors the data traffic in order to discover and protect sensitive data. • System has the ability to block or quarantine transmissions in violation of policies. • All security events are logged to a localized SIEM solution which provides early notification and the ability to retrieve data and generate reports to ensure compliance.
Vulnerability and Threat Management
• Proactive identification and audit of security vulnerabilities through continuous scanning practices conducted on servers, workstations (including devices connected to USB ports), and network devices. An array of industry-leading scanning technologies is leveraged in this process. • Rigorous patch management process that ensures the proper patches are installed, tested, and configured. • Standardized vulnerability reporting, remediation, and validation are in place.
Boundary Defense
• Secure internal network through the use of fault tolerant firewalls, protecting company resources from unauthorized access. • Intrusion prevention/detection (IPS/IDS) tools that allow the detection of possible infiltration or denial of service attacks before a compromise occurs. • Wireless networks are secured to industry standards.

DRC's Information Technology, Facility, and Personnel Security Controls

Endpoint Defense
• Aggressive endpoint and anti-virus scanning solution in place. • Endpoint and virus scanning software packages automatically update virus definitions daily and protect the following: email, servers, workstations, removable media, including any device connected to USB ports, and web traffic.
Physical Security
• Mandatory personnel key-card picture identification badges to enter and work in DRC facilities. • Mandatory visitor sign-in and temporary badges; all visitors accompanied by DRC employees. • Secure access system logs all persons entering facilities, including all after-hours/weekend activity. • Data centers are constructed of concrete floors, walls, and ceilings and meet industry standards and best practices for climate control, fire suppression, redundant network infrastructure, power and cooling, and physical security. The facility is staffed with security guards 24 hours a day, 7 days a week. • Unauthorized personnel are prohibited from entering or accessing receiving, check-in, document processing, or materials assembly areas unless accompanied by a project manager.

DRC's Security and Quality Compliance Standards

3.2. Cyberattack Protection

DRC regularly assesses new risks to the security and availability of our systems and takes proactive steps to implement new solutions required to mitigate the risks to our environment. DRC's hosting environment is configured to manage and detect cyberattacks and outside threats, including distributed denial of service (DDoS) attacks.

- All data transmitted externally, including test content and responses, is encrypted using Advanced Encryption Standard (AES) encryption.
- Test receive a unique one-time password to take a test.
- Password meets industry best practice standards for length, complexity, re-use, expiration, and log-on retry lockout.
- Accounts are only given the least set of privileges needed to perform authorized activities.
- DRC's applications secure the testing device, restricting access to other applications and the Internet as well as restricting functions such as printing, copy-and-paste, screen capture, and other similar functions that could compromise test content are blocked or cause the test to end if detected.

- All DRC workstations and servers have installed antivirus and malware detection software. Malware definition updates occur automatically, ensuring all workstations on the network can detect and quarantine known malicious software.
- Annual information security training includes information to train employees and contractors to such things as social engineering and phishing.
- Firewalls are configured to provide protection so company resources are safeguarded from unauthorized access.
- Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) detect and prevent possible infiltration before a security compromise occurs.
- Proactive monitoring for a DDoS attack and if an attack occurs, there is proactive routing of testing traffic to our security solutions partner's "scrubbing" service, which removes the attack traffic and send to DRC only the valid testing traffic. DRC runs tests with our partner to ensure that any DDoS attacks would not adversely impact performance.
- Active monitoring of system logs for malicious activity and uses a state-of-the-art Security Information and Event Management (SIEM) solution for alerting so any incidents can be mitigated quickly.
- Vulnerability scans are regularly performed of our entire environment, allowing us to verify that our patch management practices are keeping our infrastructure up to date and to greatly reduce exposure to external threats.
- Annually engage a third-party firm to conduct penetration tests on our network. These "attacks" attempt to gain unauthorized access to our network over a multiple-day period.
- Perform annual, third-party audits to ensure our security processes are properly and consistently implemented and meet industry best practices.
- Continual monitoring for changes in technology and cyberattack landscape and assessing the potential impact to DRC security posture.

3.3. DRC Employee Security

DRC has multiple measures in place to ensure the security of all testing materials and data, and to ensure that all employees, both permanent and temporary, are aware of and follow all security procedures. These measures include the following:

- All electronic files are password-protected and are accessible only to key personnel on the project. Data protection starts with a process that denies everyone access to data, and then specifically grants access to those authorized. DRC's identity and access management are managed through Active Directory, whereby users are given the lowest level of access required to perform their jobs.
- Changes in system access follow a formal change management process.

- Strong passwords—which must be unique, complex, and changed regularly—are required for all personnel to access any data. Data and electronic files are accessible only to authorized personnel.
- Access is regularly audited and immediately disabled whenever personnel leave DRC.
- Employees use key-card identification badges to enter the DRC facilities. All employees, permanent and temporary, must wear a picture identification badge. Visitors to all DRC sites must sign in and are issued badges that must be worn at all times; visitors must be accompanied by a DRC employee at all times.
- The secure access system keeps a log of all persons entering DRC facilities, including all after-hours and weekend activity.
- All employee must sign a confidentiality and security agreement and ensure privacy of all data, at all levels, at all times.
- All employees receive annual training regarding DRC's stringent security procedures. Employees are informed of requirements in areas including physical building access, employee confidentiality and behavior, data access, network and Internet access, and the safeguarding of client documents and products. Employees are also required to participate in annual Cyber Security Awareness training and complete an assessment. The assessment includes a reaffirmation agreement to maintain the confidentiality and security agreement and ensure privacy of all data.
- Unauthorized personnel are not allowed in the materials assembly, receiving, check-in, or document processing and scanning areas.

All item writers, contractors, and item reviewers must sign a statement in which they agree to treat all materials related to item development as confidential and not to disclose the content of the test materials or communication about secure information related to item development. All handscoring operations are performed at DRC's fully secure facilities, with limited access. Signed security statements are obtained from all scorers, and facilities have settings in place to prevent unauthorized duplication of secure materials.

3.4. Oversight and Governance

Ensuring that our solutions are delivered in a secure and confidential environment that meets applicable regulatory requirement is a high priority for DRC. To achieve this, DRC ensures that appropriate governance over information security risk and privacy are in place. With external and internal risks in a constant state of change, DRC continually evaluates the risk landscape and that we are complying to security and privacy requirements.

This includes risk assessment processes that evaluates new or changing threats and determines whether new controls need to be put in place or is others may need to be strengthened.

3.4.1. System Maintenance

Occasionally system maintenance and/or updates will be needed to address unexpected issues or release additional capabilities resulting in the need to deploy system change. DRC has established regular maintenance windows and coordinates these with clients as needed to ensure minimal interruption. DRC strives to make sure clients know about any update or system downtime that may be necessary in advance.

3.4.2. Vulnerability Management & Patch Management

Regular vulnerability scanning and maintaining current security patching are core principles in sound security management. DRC engages in proactive identification of security vulnerabilities through continuous scanning practices conducted on servers, workstations (including devices connected to USB ports), and network devices. An array of industry-leading scanning technologies is leveraged in this process.

Operating system vendors release monthly security patches for DRC's underlying system components and devices. Each patch undergoes an assessment to determine applicability, risk, and whether mitigating controls exist.

DRC followings a rigorous patch management process that ensures the proper patches are installed, tested, and configured. When patching is necessary, it is applied in a test environment where it is regression tested to verify it does not negatively impact performance or availability. Once regression testing completes, confirming systems are fully operational, the patches are applied to the production environment through a standardized change management process.

3.4.3. Change Management

DRC has a well-documented Change Management Standard and processes to ensure all system changes are fully documented and authorized with the express purpose of reducing risk to service interruption and/or degraded performance. Our rigorous adherence to change management helps to ensure successful implementation and support of all system.

3.4.4. System Logging and Monitoring

DRC employs extensive logging and monitoring capabilities. Some logs directly feed real-time monitoring systems and dashboards, while other logs are used for troubleshooting and forensic analysis. Monitoring and alerting occurs year-round with special attention given during peak testing windows to provide high level of system availability and performance by proactively responding to any irregularities before they can become issues. We watch for activities throughout the system and any inconsistencies trigger alerts that are investigate.

3.4.5. Service Delivery Analytics

DRC tracks the browser, IP addresses, operating system types, and usage telemetry to provide detailed performance and testing activity analytics. DRC provides a detailed program testing status dashboard to each client which provided near real-time status of all key testing activities.

3.5. Disaster Prevention, Back-up, and Recovery

All data associated with our testing programs are securely stored and backed up using DRC's standardized back-up and recovery systems. Our approach includes regular backup of data, reports, files, and systems. In addition, we have disaster recovery plans in place for recovering data in case of a physical disaster (such as fire or tornado), power or connectivity outage, or a hardware/software failure in our systems. DRC is committed to working collaboratively with clients to make sure applications are restored quickly in the event of a disaster.

DRC's disaster prevention and recovery procedures deliver contingency plans in the event of an emergency. Assessment data is protected by industry best practices for data center facilities, technology infrastructure, and security practices.

3.5.1. DRC Disaster Recovery Plan

DRC recognizes that any interruption to testing is undesirable for all stakeholders and especially to the students. To that end, we have multiple safeguards and policies in place to help deliver system availability if faced with an unexpected incident or a catastrophic disaster that causes an outage of a system or facility.

DRC maintains an active Disaster Recovery Plan to respond to unexpected outages quickly and efficiently to minimize any delays. The Disaster Recovery Plan applies to all core operations at DRC and provides guidelines for all DRC personnel when an unexpected event occurs that disrupts the normal operations of the company. The plan is kept in a secure location outside of DRC's environment and can be accessed online from any site in the event it is needed. The plan is reviewed and updated annually or as needed.

The plan is divided into three phases: Notification/Activation, Recovery, and Reconstitution.

Notification/Activation

The initial phase of DRC's Disaster Recovery Plan alerts team members to the disruption so DRC's systems can be assessed for damage. Designated personnel can activate the plan, under specified activation scenarios. Designated personnel will conduct a preliminary assessment of the incident and disseminate information on whether access to the impacted facility is allowed. This phase also activates the Disaster Recovery Plan with consideration for the scale of the incident, as well as a Disaster Recovery Log to monitor progress and updates.

Recovery

The second phase of DRC's Disaster Recovery Plan puts recovery procedures into action to mitigate any damage and interruption caused by a catastrophic event. A management control and headquarters are established, and disaster recovery teams are mobilized. Any time-sensitive disaster recovery team leads are notified of the situation, and employees, vendors, and other internal and external individuals and organizations are alerted to the situation. DRC's disaster recovery teams coordinate with management to establish responsibilities for ensuring the successful recovery of systems. Teams across DRC are assigned specific tasks to facilitate recovery.

Reconstitution

The third phase of DRC's Disaster Recovery Plan prepares procedures to facilitate the restoration of business operations. Established procedures are implemented to mobilize operations, support, and technology department restoration. Employees, vendors, and customers are also continuously updated during this phase of the process.

3.5.2. Redundant, Scalable, Flexible and Resilient Infrastructure

DRC has multiple safeguards in place to protect system hardware and to ensure that DRC's computing environment, including servers and network hardware, deliver high availability and performance.

DRC's infrastructure is highly redundant and DRC's core systems are backed up using an enterprise grade platform which ensures consistent and reliable backups. Cloud platforms also utilize an enterprise grade platform for disaster recovery and disaster avoidance. Our utilization of multiple datacenters and multiple cloud regions allows DRC to failover in extreme situations providing resiliency and redundancy for our key platforms.

Secure Data Centers

DRC's servers are housed in two highly secure data centers in separate co-locations facilities in Minnesota - one located in Chaska, Minnesota, and the other located in Minnetonka, Minnesota. These facilities are constructed of concrete floors, walls, and ceilings and are fully climate-controlled environments. The data centers meet industry standards and best practices for climate control, fire suppression, network infrastructure, power, and cooling, and physical security.

Access to the data centers is strictly controlled and limited to a small number of technology support staff. Access is controlled via government-issued ID and biometric scanners. A log is maintained documenting each time a data center is entered, by whom, and for what purpose. All server consoles are secured with tightly controlled, complex passwords.

Cloud Architecture

DRC hosts components of our solutions in a secure virtual private cloud (VPC) available in multiple cloud regions delivering high quality, reliability, security and scalability. DRC solutions are designed to be cloud-native and dynamically scalable. Each environment runs in its own instance, therefore is isolated from other environments and independently scales to the meet the demand.

Data Residency

All data collected, stored, processed, maintained, and transmitted by DRC systems resides in the United States. Data is not allowed to traverse outside of the US.

Redundancy

DRC's solutions provide multiple levels of redundancy to remove single points of failure:

- **Internet Connectivity Redundancy.** DRC leverages fully redundant Internet access using different carriers and entry points into the facilities and are configured with the capability to reroute traffic from one co-location site to the other through multiple paths.
- **Network Redundancy.** DRC has implemented a network topology that delivers redundancy for all DRC facilities in case of a network failure. Each facility has dual connections from different network providers and enter the building in separate locations delivering with multiple paths for data flow. The DRC wide area network (WAN) utilizes a redundant and dedicated private fiber optic ring in our core ring, Software Defined Wide Area Networking (SD-WAN) network capability, and Virtual Private Network (VPN), enabling high availability and recovery.
- **Data Storage Redundancy.** DRC uses storage area network (SAN) devices for maximum speed, flexibility, and redundancy in our data storage solution. Servers are connected to the SAN via redundant connections to ensure minimum interruptions due to hardware failures. The SAN allows disk space to be reallocated with ease for availability to those applications or servers as needed.
- **Web, Application, and Database Server Redundancy.** DRC servers utilize load-sharing, virtualization, and redundant power supplies, and implement RAID (Redundant Array of Independent Disks) subsystems to minimize the effect of a failed disk. DRC employs a highly redundant web, application, and database server environment. If one server should fail, the load automatically shifts to other servers. The servers are load-balanced to distribute the requests and reduce the chance of one server becoming overloaded.
- **Power Redundancy.** The co-location sites are protected against power failures. They are connected to two separate power grids, has redundant diesel generators and redundant Uninterruptible Power Supply (UPS) systems. All server and network hardware continue to function without interruption if the utility power is disrupted. The diesel generators are tested monthly.
- **Cooling Redundancy.** Cooling redundancy comes in the form of multiple cooling units; all far under maximum capacity to handle multiple cooling unit failures.

This level of redundancy and fault-tolerance form the foundation of all our platform components. If one component of the system experiences issues, the capabilities shifts traffic to other duplicate components. This sustains high availability and delivers consistent performance experience and helps to ensure that the user experience with DRC INSIGHT is uninterrupted.

Modeling

DRC has developed sophisticated modeling capability to project down to the hour by day the number of tests sessions expected allowing us to proactively put the necessary infrastructure resources in place in advance.

The model uses each assessment's testing volume projections and test windows, historical information on testing volume by day of the week and testing volume by time of day to proactively plan for expected testing volumes across all programs combined. DRC uses this data to anticipate the network, server (web servers, content servers, and application servers) and database capacity requirements, then we scale the system to support over 300% of the peak expected volume. Additionally, we conduct multiple load tests on the system at three to five times the projected volumes to validate the system exceeds DRC's and client's performance expectations.

Scalability

DRC's architecture is designed to easily and quickly scale as the demands for system resources increase. DRC utilizes a robust, virtualized infrastructure which allows for increased flexibility, redundancy, and performance. This gives DRC the ability to quickly meet the resource demands throughout testing, especially during peak testing volumes, to ensures consistent performance.

Auto-scaling capabilities are built into each service and capability we provide. Based on real-time load and incoming monitoring data, capacity will dynamically increase to handle the processing load demands. When auto-scaling is initiated, new servers are spun up and go through automated verifications before coming fully operational, allowing the infrastructure to dynamically scale to give consistent and reliable performance.

By delivering our solutions using multiple co-location data centers and multiple cloud availability zones, DRC has access to significant resources and the ability to add resources to any system to handle clients' most demanding workloads.

Monitoring

DRC employs sophisticated infrastructure and application monitoring which continually monitors real time system performance during testing. We monitor performance at all levels, from errors at a local testing site to the performance of all infrastructure components in the cloud and the data centers allowing us to respond to any anomalies before they become issues affecting performance and/or availability.

Restricted Access to Data

DRC uses an array of security technologies, including at-rest and in-transit data encryption, both hardware firewall and web application firewall technologies, industry best practice network access controls, and identify and assessment management (IAM) to manage data access authentication to restrict data access to only authorized users. All personal identity information, responses, test items, and any other data considered sensitive or subject to regulatory compliance are encrypted at rest and remain encrypted throughout any network transmissions.

3.5.3. Data Redundancy and Disaster Recovery

DRC replicates all data, systems, and components across data centers and/or multiple availability zones to maintain physical redundancy and replicas of our production environment. DRC's use of co-location data centers, secure virtual private cloud services, and elastic infrastructure services built into all our

solutions allows for physical redundancy and quick recovery if needed. The resiliency of DRC's capabilities delivers solutions designed for performance, flexibility, and availability.

Data Backup

In addition to data replication, DRC employs industry best practices for data backups. We perform regular backup of data, reports, files, and systems, including weekly backups with incremental daily backups. For databases and systems that store data with a high rate of change, we employ more granular backups that occur in real time. This gives us the ability to restore data to the specified moment in time that the issue occurred on a given day (rather than restoring to the previous night's backup).

We also conduct backups for critical components using cloud resources. Those components would be restored in the cloud, either in the same or different region.

Data is replicated between two data centers, so in the event of a disaster in which one of the facilities is lost, the other facility has the data and infrastructure required to recover and restore operations.

All data backup operations use Transport Layer Security (TLS) encryption when transmitting the data both internally and externally. All the data backups employ data at rest protection using Advanced Encryption Standard (AES) 256-bit encryption algorithm.

Disaster Recovery

DRC has developed a disaster recovery strategy that leverages a dual data center facility and cloud-based services architecture. The recovery procedures for both the automated services and manual actions exist in disaster recovery runbooks and regularly reviewed, version-controlled and kept up to date.

3.5.4. Data Retention

DRC establishes a data retention plan with each client that governs how long various types of data are retained and when the data should be deleted and/or destroyed.

DRC will comply with destroying the active data on our systems; however, deleting data from backups is cost prohibitive. In the remote event that a restore from a backup is required after the active data is removed, DRC will purge any records from the restored data as required to meet this commitment.

3.6. Security Incident Management & Response

DRC has a documented Incident Response Standard. This standard is implemented by DRC's Incident Response Team, which is composed of various IT professionals throughout the organization.

The Incident Response Standard provides guidelines for responding to and recovering from a security event. Responsibilities and procedures are fully documented for the Incident Response Team. These include procedures for:

- Monitoring, detecting, assessing, and classifying security events

- Response, escalation, recovery, and tracking
- Documentation, communication, and reporting
- Collection, protection and preservation of relevant system and application information, and other relevant evidence pertaining to the event for future forensic and applicable legal requirements
- Post-event review for process improvements for prevention, early detection and remediation

The Incident Response Team meets a least annually to discuss and improve on policies, procedures, and lessons learned from past incidents. The team also conducts training exercises and testing. The goals of the incident response team are to maintain or restore business continuity; defend against further attacks; perform counter-intelligence and intelligence activities where appropriate; and deter attackers through investigation and prosecution.

3.6.1. Incident Detection

DRC utilizes both an Intrusion Prevention System (IPS) and Intrusion Detection System (IDS). DRC has guidelines for intrusion detection implementation, along with associated personnel roles and responsibilities. This system covers every host on the network and the entire data network. DRC's IPS and IDS are responsible for monitoring all host- and network-based intrusions. These systems are tuned to minimize false positives and configured to alert on high-priority events.

Intrusion detection logs are sent real-time to the DRC SIEM system. Any suspected intrusions, suspicious activity, or unexplained, erratic system behavior alerts from the SIEM, as well as by any other administrators, users, or computer security personnel, are immediately reported to the Incident Response Team. The Incident Response Team then takes immediate action to minimize damage, remove any hostile or unapproved software, and recommend changes to prevent future incidents. Actions are based on DRC's Incident Response Standard.

3.6.2. Incident Response

In the event of an incident, DRC's primary goal is to maintain or restore business continuity, so early detection and containment of a security incident is vital. Following containment, steps are taken to remediate any issues resulting from the event. Once the incident is resolved, analysis of the incident along with executive and technical reports are prepared that document the impacts, actions taken, and recommendations to prevent further occurrences.

4. DRC'S ASSESSMENT DEVELOPMENT AND PRODUCTION SECURITY MEASURES

4.1. Item and Test Development Security

The maintenance of test security for the program throughout the item development process is essential given the nature of these high-stakes assessments. Item and form security continuously punctuate every phase of DRC's test development process. DRC takes necessary precautions to implement and preserve the integrity of test items by maintaining the security of the physical environments, electronic environments, and file transfer processes.

- **Electronic Security**—Test items, test materials, electronic files, data files, answer keys, and other program data are managed within a secured network environment. Data and electronic files are accessible only to authorized personnel. Passwords, which must be changed regularly, are required for all individuals with access to data. A full array of security technologies, including audit trails, firewalls, intrusion protection, source-code security, and secure file transmission via Secure Sockets Layer (SSL) further protects test and item data.

- **Item Writers, Contractors, Item Reviewers**—All item/passage writers, contractors, and reviewers for the program must sign a statement in which they agree to treat all materials related to item development as confidential and not to disclose the content of the test materials or communication about secure information related to item development.

- **Physical Document Storage**—During the item and form development processes for the program, all hardcopy materials related to item and form development are stored in secure locations when not in use. After review and delivery of items or printer's proofs, all item and form development materials are boxed for security purposes and final storage. Only authorized staff are granted access to secure materials. Document retention is based on the client's security policy requirements and includes storage in an environment that is secure from access by the general public or unauthorized personnel. Item and form development materials remain secure until the client provides written authorization to securely destroy hardcopy materials.

- **Desktop and Laptop Computer Security**—All item and form development work is done either on hardcopy or directly in DRC's electronic item banking system (a server network system), eliminating the need to store item and form information on individual desktop or laptop computer hard drives. All information, including item and form images that are stored in the item banking system on the network, is protected by comprehensive security controls. All hardcopy materials are protected via DRC's physical document storage procedures, discussed above.

4.2. Electronic Item Bank Security

DRC's electronic item banking system, Item Development and Educational Assessment System (IDEAS), patent pending, is protected by password assignment and a sign-in process that authenticates users based on each person's role for the project. Authorized users are provided access only to portions of IDEAS pertinent to their roles. For example, mathematics test development specialists may not be allowed to view science items, while others may be restricted to read-only access. Electronic item and form information stored in IDEAS remain secure until written authorization has been received from the appropriate client contact to securely delete all such information.

4.3. Security Processes for Item Review Sessions

DRC recognizes the importance of maintaining security of all items, prompts, and student responses. No secure materials are ever released to participants in item review sessions before meetings.

Signed security agreements are required from all item review session participants and these agreements are retained for the duration of the contract. At the beginning of all new content or data review meetings, each participating reviewer is asked to sign a Confidentiality Agreement that specifies

state confidentiality agreements and security regulations. The Confidentiality Agreement also outlines ownership regulations for the program. No confidential material is released without prior approval.

During review meetings, DRC test development specialists (facilitators and recorders) monitor the security of all items, passages, and testing-related materials throughout the entire process, making sure none are left unattended. All materials sent to meetings are sent through a secured mailing process and have tracking documentation. Each set of materials used during the meetings are numbered so that any missing material are immediately noted when materials are checked in and out each meeting day. DRC prohibits the use of personal computers and cell phones in meeting rooms. Our staff is vigilant about maintaining security at these meetings. Materials are either disposed through the use of on-site shredding bins or securely shipped back to our test development facility in Plymouth, Minnesota, where they are securely destroyed.

4.4. Test Publication Security

DRC's Document Services Division incorporates our complete in-house Printing Department and Document/Graphic Design Group, which produces and prints scannable forms and other testing materials from typesetting to editing and printing. DRC's Document Services Divisions follows the same strict security standards and policies as the rest of the company, and test publication takes places in our secure facilities.

When outside printing vendors are used, DRC selects only printing vendors that have great sensitivity to state testing requirements and timelines and that have previous experience with printing educational testing materials. Each external printing vendor is required to maintain the strictest level of security during the production of materials and is asked to sign a security affidavit attesting to their commitment to this security before documents are submitted to them for production. All DRC vendors, including printing vendors, are fully vetted and carefully monitored for security measures and performance as a part of DRC's Vendor Management Program. Security practices are documented and embedded into DRC's ISO 9001:2015 certified processes that span the entire chain of custody of testing materials.

4.5. Secure Materials/Test Booklet Security

DRC employs the following test booklet design features to ensure security:

- **Unique Barcodes:** The use of barcode technology maintains an accurate account of all test booklets. DRC generates a unique security code that is pre-printed on each secure document. The barcode also ensures that each student response document returned to DRC for processing and scoring can be unequivocally associated with only one record in a master database. Requirements and printed documents are subjected to strict quality assurance inspections to ensure accuracy. The format and precision of the printed information are closely examined by DRC's software quality assurance analysts to make certain the information is correct.
- **Security Seals:** Security seals manage when and how specific sections of tests are released to the students, such as with writing prompts, and to control administration of certain sections that require specific testing criteria, such as non-calculator mathematics sections. DRC uses

security seals on test booklets to ensure students do not have access to test content prior to test administration sessions.

- **Shrink-Wrapped Test Booklets:** While shrink-wrapping test booklets in packages assists with distribution and helps ensure equitable distribution of test forms within classrooms, shrink-wrapping also secures test content until preparation and distribution of the test booklets by test coordinators and test administrators.

5. DRC'S TEST ADMINISTRATION SECURITY MEASURES

5.1. Assessment Portal

DRC's web-based assessment portal, DRC INSIGHT Portal, provides users with access to the various administrative tools and functions necessary for the management and administration of the program. This secure, permissions-based system employs role assignments to ensure a user can only view or edit data for which he/she is authorized. Users must log in with a unique user ID and password to gain access to the system.

5.2. Materials Tracking

Operations Materials Management System (Ops MMS), a proprietary and innovative system that uses barcode and scanning technology, provides an accurate and efficient method for tracking secure materials throughout packaging, distribution, collection, materials receipt, and check-in. For packaging and distribution, Ops MMS identifies all secure test materials by site code and provides an automated quality check between items designated for a site based on the following: Name of Testing Program, Site, Grade, Subject, Material Type, Quantity, etc. For materials receipt and processing, Ops MMS provides data on actual versus expected receipts, along with used versus unused student answer documents. Ops MMS also generates missing materials reports early on, so that any missing materials can be immediately resolved.

5.3. Secure Distribution and Collection

Shipping vendors used by DRC are fully vetted and carefully monitored for security measures and performance as a part of DRC's Vendor Management Program. Security practices are documented and embedded into DRC's ISO 9001:2015 certified processes that span the entire chain of custody of testing materials. DRC's shipping vendors for most of our products use controlled access where only authorized personnel can enter facilities, consolidation points, and distribution centers. Our shipping vendors provide real-time shipment tracking and proof of delivery, completing the distribution chain of custody process. DRC's logistics experts carefully coordinate and monitor distribution activities of all shipments.

5.4. Secure Materials Receipt

Secure materials check-in and processing occurs immediately upon receipt of testing materials. DRC Operations staff provides real-time feedback on actual receipts versus expected receipts for sites. This allows for immediate communication with sites regarding any materials receipt "shortfall." This processing system provides quality control measures that are specifically related to potential test security issues, and problems can be detected early. Secure materials issues are identified and resolved

before any reporting takes place. DRC's IBML image scanners and Image Scoring System also allow for on-demand retrieval of specified images (e.g., specific batch files, specific grades, specific students); each image is assigned a unique identification number that allows for quick and easy retrieval at the various site levels.

5.5. Secure Materials Storage

Upon completion of processing, scannable documents are boxed for security purposes and final storage at DRC's secure storage facilities. Our storage facilities are also climate- and pest-controlled, allowing for the preservation of the documents. All student response documents that are returned from sites are securely handled and stored. Individual student tests (original hardcopies) are easily retrievable because of DRC's effective document storage procedures, which is a critical requirement for thorough and appropriate investigations of potential security compromises. Materials are securely destroyed only after written authorization is obtained.

5.6. Site-Level Security

DRC's Site level security policies manage and protect information at every level of processing and in every system component. Our procedures and recommendations address awareness, prevention, and detection/response, and are based on our extensive experience in test security as well as knowledge around industry best-practices.

- **Training and Information:** One of the most critical pieces of secure test administration is conveying test security information to test administrators, as well as any other individuals assisting with testing. DRC collaborates with the client on preparing and presenting training materials and webinars, including recommendations for continued enhancements throughout the contract period as issues arise or new protocols or technologies emerge. These training and informational needs include:
  - — Identifying all secure materials as "secure."
  - — Communicating that all student work is confidential and secure.
  - — Providing detailed test security information in all manuals and informational materials.
  - — Providing test security training or training overviews in manuals to encourage the formal training of all local staff.
  - — Communicating that data forensics analyses are routinely conducted as part of each administration.
  - — Clearly specifying all activities that constitute compromises of security and identifying the individual and wide-ranging repercussions associated with a test security compromise.
- **Security Checklists:** These pre-printed forms are critical tools for tracking and accounting for secure materials at sites before, during, and after test administration. DRC provides these pre-printed forms for reference and use by test coordinators to assign, check-in, and verify return and accountability of secure test materials before, during, and after test administration. Each security checklist includes a list of the security barcode numbers of all secure materials assigned

to the site. The secure materials are listed in ascending order by product. The checklists provide space for test coordinators to document secure material distribution and return.

- **Test Security Certifications:** DRC can provide certificates to promote and help ensure compliance with the test security procedures established by the client. It is the test coordinator's responsibility to distribute and collect the test security certifications. DRC works with the client to develop procedures for collecting, storing, and/or reporting these forms after each administration.
- **Communications from Clients:** DRC's customer service database allows DRC to collect information related to specific communications (telephone conversations, emails, faxes, etc.) and correlate these communications. This provides DRC with an excellent tool to track potentially problematic situations or document references to possibly inappropriate activities regarding test security (e.g., references to specifics in test booklets). Our database also provides documented evidence related to any suspect activities.

5.7. Online Testing System Security

DRC recognizes that ensuring security is of the utmost importance in maintaining the technical quality, perceived fairness, and integrity of any testing program. DRC has integrated security features and procedures throughout the DRC INSIGHT system to ensure security for all aspects of the assessments.

5.7.1. Secure Student Access

Students are required to provide a valid username and password to access the online testing system. The test administrator provides each student with a Student Test Login Ticket, which contains the student's username and a unique, pre-generated password. A separate, unique password is generated for each assessment, ensuring that **students can only access the test they were assigned**. Passwords are generated by combining a common four-letter word with a random four-digit number. Test Tickets are generated from within the secure educator portal, which is pre-populated with student records. As an additional security measure, upon logging in, a Student Verification Page prompts the student to verify their profile information, including any assigned accommodations, prior to initiating the test. The student's name is also displayed on the screen during the test, providing an additional verification check for the student and the test administrator.

Because login tickets are secure material, they should be printed as close to the date of testing as possible and kept secure until given to the test administrator for distribution.

5.7.2. Secure Administrator Access

The administrative portal provides tiered, permissions-based access for all state, district, and school staff involved in the administration of the assessments, including test coordinators, test administrators, state personnel, and any other staff needing access to the system. These functions are controlled through **a variety of security levels to ensure a user only views or edits data for which the user is authorized**. Users must login with a unique user ID and password to gain access to the portal in order to administer tests, view/maintain student data, and access student performance reports. The system

automatically enables or disables access to specific functions based on the user's profile and permissions.

High-level administrator accounts control the permissions and the level of access relative to each sub-user. The DRC INSIGHT portal is a permissions-based system, meaning that users with administrative rights need to select what role a sub-user has and assign permissions to that individual. This allows the flexibility for users to have the same roles but different permissions. Each district can set up users with as much or as little permission as deemed necessary. A user's role and permission may be modified at any time.

To promote the security and confidentiality of student data, new DRC INSIGHT portal users are prompted to review and agree to a security and confidentiality agreement upon logging into the system for the first time. The user agrees not to disclose any student information from the system to anyone other than a state, district, or school official as defined by the federal Family Educational Rights and Privacy Act (FERPA).

As an additional security feature, if a user account is inactive for a pre-determined period of time, the account automatically expires and must be manually reset.

5.7.3. Security of Test Content and Student Data

In high-stakes assessments, security of test content and student data is of paramount importance. Throughout all data transfers—from the student testing device, across the Internet, to DRC's databases and back—test content and student responses are secured through a combination of methods.

Methods to Secure Test Content and Student Responses

- Use of kiosk mode and other device-specific settings to secure the student testing device
- Use of industry standard encryption technologies for encrypting data
- Use of Secure Sockets Layer (SSL) protocol through Hypertext Transfer Protocol Secure (HTTPS) for securely transmitting data

Test content is encrypted at the host server and remains encrypted throughout all network transmissions; content is decrypted only once the student login is validated. Decrypted test content on the testing device is stored only in memory during each test session. Once the session is ended (the test is completed, or the student logs out), computer memory is purged to ensure security of test content is maintained.

When the DRC content hosting service is used, test content is stored locally within a school or district's network. All data that is transmitted to and from the hosting service is encrypted in transit and storage. Test content is only decrypted once it reaches the student's computer and the student login is validated. Only authorized users are allowed access to the content hosting service.

Student data, including personally identifiable data and testing responses, is always encrypted. DRC encrypts data both at transit and at rest, further protecting the security of students who are testing.

5.7.4. Security of the Testing Interface

The following features of the DRC INSIGHT testing interface ensure that test content is not compromised during testing.

- **Device Security:** DRC INSIGHT creates a secure environment for all student testing devices during testing. The system also blocks access to other applications and websites, prevents interference from automatic software processes such as virus scans, and secures the device to prevent compromise to the test content. Security is device-specific:
  - For desktop computers and laptops (Windows, mac OS, and Linux), the system uses "kiosk mode" to secure the testing device. If two monitors are connected to the device, the system automatically inactivates the second monitor while in testing mode.
  - For iPads, the system uses Apple's iOS Automatic Assessment Configuration (AAC) to automatically configure the iPad for testing. This allows the testing app to lock the iPad into a "single app mode" when it is launched, which prevents the student from using any other apps while testing.
  - For Chromebooks, our system runs in Single App Kiosk Mode to secure the device properly.
- **Prevention of Test Submission from Multiple Machines:** This feature prohibits two students from using the same login at the same time. When more than one login is detected, a warning message appears, and the student is directed to ask for assistance.
- **Pause Feature:** Students may pause testing if a short break is needed (e.g., restroom break). Once a student clicks the Pause button, the current test item is removed from the screen to ensure the security of the question and answer. If a test is paused and not resumed within the same day, the test is locked, and special intervention is required to unlock the test so the student can resume the test.
- **Inactivity Timeout Feature:** The system times out and closes the test after a defined period of inactivity (e.g., no mouse movement or typing for 20 minutes). The length of time is configurable. The application displays an inactivity countdown clock and timeout warning message prior to logging the student out of the test and closing the application.

5.7.5. Procedural Security

DRC provides training and documentation to test coordinators, technology coordinators, and test administrators to ensure consistent security measures are implemented and followed during online testing. Standardized testing procedures ensure all students are tested under similar conditions in all classrooms.

Manuals for assessment coordinators and administrators thoroughly document security procedures for test administrators to follow during online testing. In addition, security procedures are reviewed during DRC-led training sessions with assessment coordinators and technology staff.

5.8. Monitoring and Addressing Test Administration Security Compromises

DRC provides multiple methods for monitoring and investigating the security of both online and paper test administrations.

- **Irregularity and Data Forensics Analysis:** DRC is able to provide a comprehensive data forensics and monitoring program that can be seamlessly integrated within assessment and accountability programs. There are two windows of opportunity to look for behavior that may indicate that the standardized test administration and security procedures were not followed. The first opportunity is during the testing window. Reports are available through the online portal to help identify instances such as unusual amounts of logins or start times. The second opportunity is after the testing window when data collected during the testing window is available for analysis.
- **Online Testing Status Reports:** DRC provides online testing status reports monitoring the security of online test administrations. These reports allow district and state users to track testing activity for a given test administration. The purpose of these reports is to provide state and district users with tools to monitor and research unusual login patterns that occur during the administration of online assessments.
- **Documentation of Potential Test Administration Security Compromises:** In any instance of a suspected compromise of test security administration, DRC staff document the communication or circumstance and immediately notify DRC's Project Management Team. The Project Management Team reviews the documentation and swiftly notifies clients effected by the issue, providing as much documentation as possible. DRC does not address potential test security compromises with district staff; DRC considers the sharing of inappropriate information with any district, schools, parents, the media, etc., to be a breach of our commitment to client confidentiality. DRC provides support to clients as they address any potential test security compromises within districts.

6. DRC'S SCORING, REPORTING, AND DATA SECURITY MEASURES

6.1. Processing and Scanning Security

All processing and scanning occur at DRC's fully secure facilities. DRC maintains stringent security and quality control procedures during scannable answer document processing. client-approved processing and scanning procedures provides our Document Processing staff with step-by-step instructions to follow during scannable answer document processing. DRC's software quality assurance staff performs extensive tests to ensure all scanned data are captured and securely and accurately stored in a secure database environment. Student responses and data are kept confidential and secure at all times. Our use of barcoding technology allows us to score and accurately link student response data and images without the inclusion of student names, birthdates, or other personal identification information. All client and student demographic and response data are protected by stringent security features and procedures within DRC's secure computing environment.

6.2. Handscoring Security

All handscoring performed by DRC occurs at DRC's fully secure facilities. Access to all scoring facilities is limited to staff and to visitors accompanied by authorized personnel. DRC staff discusses security guidelines and obtains signed security agreements from all scorers. DRC retains these agreements for the duration of the contract. To prevent the unauthorized duplication of secured materials, scorers are not able to print from their computer workstations without authorization by management. Additionally, workstations at the scoring centers do not have access to the Internet. DRC's scorers fully understand that no testing materials may leave a scoring site.

6.3. Electronic Scoring Security

Electronic scoring is managed securely through the use of the DRC INSIGHT Portal and utilizes a user's secure log-in information. Access to the program is restricted to users without prior-approved permissions, ensuring that data remains private and secure. The portal also controls the functions that any given reader or supervisor can perform. Access to scoring projects is controlled via DRC's Reader Team Management.

6.4. Student Confidentiality

Our systems and processes are designed so that all data is secure at all times. Procedures are frequently verified to confirm adherence. Where applicable, procedures are embedded into the process so that they must be followed. All DRC staff members receive training on our student confidentiality requirements. Only authorized personnel have access to electronic databases and networks. All DRC project managers are versed in security and privacy policies and are required to escalate privacy/security issues immediately.

DRC ensures that all student data remains confidential and secure. Individual student reports, data records, and any transmittal media is distributed only to the appropriate entity upon approval of the client. DRC carries out all processing, scoring, and reporting of test results in a manner which does not permit the personal identification by individuals other than representatives of DRC. Barcoding technology allows us to score and accurately link response data and images without the inclusion of student names, birthdates, or other personal identification information. All sample reports and data files provided to the client are carefully developed to exclude names. Mockups and samples are provided with a nonspecific identifier (e.g., Student 01).

6.5. Data Management Security

In our computing environment, DRC utilizes security controls that relate to our hardware, data, and network. DRC manages multiple terabytes of client data; therefore, security is an inherent, inextricable, and indispensable component of our business. DRC enforces strict security measures to prohibit unauthorized personnel from gaining access to assessment and client data, including personally identifiable information (PII), through either deliberate or unintentional action.

Our company-wide measures address the full range of security, including computing environment, physical building access, employee confidentiality and behavior, and the safeguarding of client information, documents, and products (please see above for detailed information). These physical and

computing security procedures are in effect 24 hours a day, 7 days a week. This allows us to provide secure maintenance and storage of student and assessment data files, even when not in use. For our programs, data are captured and stored on a secure, protected server. Access to the data is only be granted to those DRC employees who are working directly on data-related tasks associated with the program.

DRC incorporates rigorous quality assurance activities throughout the process to ensure data quality, integrity, and security. Prior to any test materials returning to DRC, the software quality assurance staff performs extensive tests to ensure all scanned data and selected-response items are captured and accurately stored in a secure database environment.

We recommend that electronic results data transfers to and from clients be done via a secure, password-protected SFTP site established and hosted by DRC. Separate user IDs and passwords are created for each client-approved individual who requires access to the site. All files posted to the SFTP site are encrypted. DRC works with each client to confirm data exchange procedures are secure and appropriate.

6.6. Reporting Security

DRC's security practices extend to keeping our client's data related to reporting secure. This includes distribution of hardcopy reports, posting reports and data to our secure web-based reporting tools, or any other type of reporting medium. No reports, documents, or data files containing secure information are released without prior written approval from the client.

Hardcopy reports are packaged and clearly labeled so they can be securely and easily distributed. DRC uses only shipping vendors that provide online tracing and tracking services, such as United Parcel Service (UPS). In addition, DRC's Project Management Team monitors the delivery schedule of reports. Each ship-site is required to sign for its report shipment. DRC tracks each delivery and compiles a record of each signed-for shipment. If a shipment is not delivered within the expected window, DRC's Logistics Team contacts the shipper and traces the shipment, providing an update and resolution to the client.

For electronic delivery of test data and results, DRC utilizes secure data and file transfer processes. For clients choosing to use DRC's secure, web-based reporting systems, we require unique user IDs and passwords to ensure confidentiality and security. During log-in, the user ID and password are authenticated prior to allowing the user to view reporting results. Each user, based on user ID and role, receives privileges that are restricted to client-specified levels of access (i.e., school, district, state). DRC employs Secure Sockets Layer (SSL) for all data transferred over the connection.

7. DRC'S SECURITY REQUIREMENTS FOR SUBCONTRACTORS AND VENDORS

DRC holds our supply partners to the same high standards we hold ourselves. Partner companies and vendors are only granted access to data that is necessary to fulfill their role on the project. Access is restricted and monitored to ensure data always remains secure. All vendors are fully vetted and carefully monitored for security measures and performance as a part of DRC's Vendor Management

Program. Security practices are documented and embedded into DRC's ISO 9001:2015-certified processes that span the entire chain of custody of testing materials and data.

DRC's Vendor Management Program encompasses the following:

- Defines a set of DRC process specifications and other business requirements we expect our supply partners to meet.
- Requires a written response that is a confirmation of compliance, a submission of supporting documentation, Interconnection Security Agreement (ISA), a Non-Disclosure Agreement (NDA), and/or a DRC Vendor Management Questionnaire.
- Utilizes an onsite business process assessment where DRC Security, Procurement, and Quality staff members audit key supplier business processes, as required.
- Conducts monthly and annual business reviews of supplier performance (reviewing performance requirements around quality, delivery, and overall service). When necessary, corrective action plans and follow up sessions are also included during these reviews.

To ensure we are complying with our vendor management and security standards, DRC has embedded security documentation within the DRC Quality Management System. All vendors are audited as part of DRC's Vendor Management Program. These ISO-certified quality practices are audited several times a year by DRC Internal Audit staff and a third-party assessor.