D3 SECURITY ☎ 1-800-608-0081 www.d3security.com ✉ sales@d3security.com

D3 SECURITY

INFORMATION SECURITY RFI

Document No.	Version 6
Last Revision Date	10th December 2021
Date Implemented	10th December 2021
Next Review Date	14th December 2022
Responsible Person	Stan Engelbrecht
Approver	Gordon Benoit

SECURITY OVERVIEW

The President, VP of Development and the Senior Developer are the authorities that maintain the information security policy.

No D3 personnel have access to the physical environment where the data is hosted. As per D3's internal security policy, only the following people have electronic access:

GORDON BENOIT
D3 Security
President

MIN LU
Vice President
of Development

JERRY YU
SR Application Developer
and Installations Lead

With the growth in mobile computing and other forms of network communication, there are increased risks associated with working from environments that are removed from the four corners of the physical office. Mobile computing is using equipment such as tablets, PDAs and laptops to connect remotely to an organization's internal network and systems.

Remote computer usage may only be used with the authorization of IT Asset Management. A mobile user CANNOT connect to the D3 Security Management Systems Inc. server or SaaS environment from unauthorized locations, using different mechanisms, or via portable devices such as tablets, PDAs, laptops and mobile phones. Server and SaaS access is restricted by D3 Security IP and VPN controls. Organizational charts are in place to communicate key areas of authority and responsibility. The Security Responsibility Policy provides structure delineating individuals' responsibilities related to security.

THE SECURITY RESPONSIBILITY POLICY

- **VP of Development**
  Information security
- **Senior Systems Engineer**
  Administering user accounts and authentication management.
- **Information Security Manager**
  Creating security policies and procedures.

  Monitoring and analyzing critical security announcements.

  Distributing information to appropriate information security and business unit management personnel.

  Creating and distributing security incident response and escalation procedures.

  Monitoring and controlling all access to data.

For clients with PCI or HIPAA/HITECH requirements, firewall configuration standards include requirements for a firewall at each internet connection, between any DMZ, and the internal network. The servers are deployed in Microsoft Azure data centers to fulfill a variety of roles (e.g., web server, database server, firewall, etc.). D3 Security's specialties include high-availability database hosting for market-leading relational databases and high availability enterprise cloud solutions based on VMware ESX servers.

D3's hosted solutions provide failover, restoration and rollback support 24 hours a day, seven days a week. D3 Security also helps facilitate high availability and redundancy using VMware and other cloud technologies, enabling applications that do not have a redundant configuration to be more highly available by moving virtual servers between physical computing resources in the event of hardware failure. D3 Security uses configuration management, auto-scaling, and other automation in cloud architectures that achieve a client's desired level of resilience or high availability across multiple Microsoft Azure availability zones and regions. D3 utilizes Azure Geo Redundancy Storage for Primary and Secondary Zone backups. D3's Recovery Point Objectives (RPO) < 1 hour and Recovery Time Objectives (RTO) < 24 hours.

RISK ASSESSMENT AND TREATMENT

The risk analysis methodology and approach is conducted using guidelines in NIST SP 800-30 Revision 1, Risk Management Guide for Information Technology Systems and NIST SP 800-39 Managing Information Security: Risk Organization, Mission, and Information System View. The assessment phase includes identifying organizational areas supporting clients through an entire lifecycle of services with D3 Security. This phase identifies major business processes to be included as part of the analysis in addition to the management network components that are used in direct support of clients. Once the organizational and mission/business threats and vulnerabilities are identified, management will convert the vulnerabilities into risks based on categorizing the likelihood of vulnerabilities being exploited, mitigating controls, and the possible business impact. The Risk Analysis team analyzes the effectiveness of controls for maintaining good governance at the corporate level and for meeting availability and security objectives for clients. Management will determine the overall likelihood rating indicating the probability that a vulnerability (technical or organizational) could be exploited by a threat-source (internal or external) given security and other controls in place, as well as the adverse impact resulting from a threat successfully exploiting a vulnerability.

The result of the risk assessment process is a body of recommendations to safeguard D3 Security as a corporate entity, its information systems, and the information systems of the clients for whom D3 provides services. Management has implemented a Risk Management Policy, which requires the Company to conduct an annual risk assessment to identify threats and vulnerabilities and ensure the confidentiality, integrity and availability of D3 Security's clients' systems. The Risk Management Policy and other information security policies are reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

ASSET MANAGEMENT

The majority of D3 Security' hosting services are provided by Microsoft within Azure East and Azure West regions. Logicworks provides 24-7-365 infrastructure monitoring for D3 as a service and employs Alert Logic as its vendor of choice for Malware/Antivirus protection, continuous vulnerability scanning, and web application firewall services.

Accounting for D3 Security Management Systems Inc. corporate assets assists in providing adequate protection for them. All assets have an owner, certain technology assets are centrally owned and other assets are owned within the business unit.

D3 Security utilizes antivirus software on all Windows-based desktops and laptops, Linux servers, and within Microsoft Azure. Definition updates and scans are performed on a daily basis, with exception-based scan reports sent to senior system engineers. All anti-virus (“AV”) solutions are centrally managed and cannot be disabled by users.

PERSONNEL MANAGEMENT

D3 Security performs background checks on all employees prior to hiring and granting them access to system components. Staff members with security breach responsibilities are periodically trained. In addition, there are periodic meetings where the team will discuss incident response to transfer knowledge and conduct training. D3 Security employment candidates agree to the submission of background checks. D3 Security uses a 3rd party background check organizations to perform background checks. It is at D3 discretion to deny or terminate employment due to information discovered through a background check.

D3 Security utilizes a multi-faceted approach to ensure that existing policies and procedures are consistently being followed by all employees, summarized as follows:

- Written policies and procedures provide a source of reference and guidance
- Staff training, both internal and external, ensures that all employees are aware of the relevant policies
- Checklists are required to be completed to ensure required steps are performed

USER ACCESS MANAGEMENT

The Access Authorization Policy addresses the safeguards for granting and authorizing appropriate access to client systems. Formal written job descriptions exist for positions with key functional groups to support segregation of duties. Checklists for newly hired and terminated employees are formally documented in the Company’s policies and procedures. Access to the outsourced data center facilities is limited to authorized personnel. The President, VP of Development and the Senior Developer are responsible for submitting authorized requests to the data center facilities utilizing the data center provider’s website.

D3 DBA ACCESS MANAGEMENT

Access to D3 hosted client environments is restricted to Sr. D3 Database Administrators (DBAs) and requires client consent and notification. The D3 DBA's must then connect to Azure cloud via VPN followed by a Multi-factor Authentication process. The D3 DBAs have no access to the application itself only the database. This access is logged and monitored by Alert Logic and reported on daily via Logicworks' staff. Access logs are reviewed weekly by D3 SR. DBAs to ensure accuracy and to verify the legitimacy of the logs. D3 DBAs have their access reviewed Semi-annually by the VP of Development to ensure proper segregation of duties and that access controls are properly in line with company policy.

USER PASSWORD MANAGEMENT

Management has implemented group policies to enforce strong password controls and workstation lockout settings. D3 Security users requiring access to client infrastructure as a part of their responsibilities use unique passwords where possible for access. When root or administrator credentials are required, users have unique accounts within the PMP password manger system.

PASSWORD COMPLEXITY REQUIREMENTS

D3 follows the NIST 800-63 Revision 3:
Digital Identity Guidelines
The major recommendation is the utilization of passphrases as opposed to a password. Please refer to D3 Password Policy for more information.

Passwords are changed every 90 days, or 30 days for administrators. Successful and unsuccessful employee access attempts to PMP are logged and reported to the PMP administrator. For managed Azure and AWS, D3 Security has configured SSO with a MFA token for unique user identification. There is a lockout threshold of 5 attempts, which can be changed by the administrator. Only the administrator can unlock an account. The manager is also notified of the incident. D3 Security uses centralized authentication for management systems which further restricts access to resources by organizational units related to users' job functions.

CRYPTOGRAPHIC CONTROLS

Data is encrypted in transit on external public networks, including the Internet. HTTPS via TLS 1.2 is required for all data in transit to and from the D3 application. Data is also encrypted in storage on servers, e.g. databases and file-servers. D3 uses AES256 to encrypt required field data and attachments. The encryption key itself is also encrypted by AES256. D3 uses AES256 to store passwords in an encrypted format.

APPLICATION SECURITY AND CONFIGURATION MANAGEMENT

D3 software is an ASP.NET web application; we follow Microsoft Secure Coding Guidelines and comply with OWASP Secure Coding Practices. Our QA team also conducts Penetration Testing on our application to ensure its security. D3 does not use any third party application components, further reducing application security risk. The D3 platform is one application composed of multiple modules. Each module and its documentation are updated quarterly. This is inventoried within the development department.

Alert Logic conducts continuous scanning of the network and infrastructure housed with D3's Azure environment the findings are ranked based on CVSS. The findings are reviewed by the Information Security Manager and other engineers to validate findings and prioritize further actions. The IT Department maintains an up-to-date listing of all operating systems and the respective level, version, and patches that have been applied. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures.

INCIDENT MANAGEMENT

D3 follows NIST 800-61 rev2 for all Incident handling processes. D3 Security has a process to improve upon incident response plans according to lessons learned from incidents and to incorporate industry developments. D3 Security conducts periodic meetings with the Logicworks Incident Response Team to discuss any updates to the environment or the Incident Response Plan.

SECURITY AUDITS

D3's Managed Security Provider, Logicworks is SOC 2 type 2 certified. Audit trails and related logs are located on centralized servers. Access to these trails and logs are restricted by job functionality. Currently, only Senior NOC and Operations Management may access these. Access is controlled via ACLs. System and security logs are maintained on log aggregation server, as well as collected and proactively monitored via Alert Logic Log Manager within the Azure environment. Logicworks is alerted to risks, threats and activity via the monitoring system of these devices. These alerts will come in the form of email and/or direct phone contact from Alert Logic depending upon the severity of the threat or incident.

TRAINING & AWARENESS

D3 Security's Security Awareness training materials provide guidance to employees on how to guard against, detect, and report malicious software. D3 Security staff undergoes training annually related to security policies and procedures. There is an annual awareness sign-in roster sheet for the employees to sign. Staff members with security breach responsibilities are periodically trained. In addition, there are periodic meetings where the team will discuss incident response to transfer knowledge and conduct training.

BUSINESS CONTINUITY AND DRP

D3 Security has a Contingency Operations Plan in place, which documents the procedures to allow facility access while restoring lost data in the event of an emergency such as manmade or natural disasters. The majority of D3 Security's hosting services are provided by Microsoft within it's Azure East and Azure West data centers, which obtain their own SOC reports.

DECOMMISSIONING STRATEGY

D3 Security uses a secure wipe program that adheres to the NIST 800-88 standard to sanitize all electronic media prior to media re-use at the hosting provider's location.

In D3, Sensitive paper based information is controlled and destroyed by paper shredders.

AZURE FIREWALL SERVICE

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources.

Azure Firewall includes the following features:

- Built-in high availability
- Availability Zones
- Unrestricted cloud scalability
- Application FQDN filtering rules
- Network traffic filtering rules
- FQDN tags
- Service tags
- Threat intelligence
- Outbound SNAT support
- Inbound DNAT support
- Multiple public IP addresses
- Azure Monitor logging
- Forced tunneling
- Web categories (preview)
- Certifications

BACKUP MANAGEMENT

D3's customer database is backed up every 15 minutes to another region. In addition, all the application and workloads are replicated to the DR region as well. We test the restoration activities in our environment at least once a year. The new engineers that join the DRP of D3 team undergo the DRP training and required to restore the services themselves. The restoration can be done between 2 to 24 hours of the incident depending on the complexity.

CHANGE CONTROL AND PATCH MANAGEMENT

The Change Control Procedures, Vendor Patching Policy and the Vulnerability and Patch Management Policy address the assignment and key activities and controls associated with the change management processes for hardware and software. Sections of the policies regarding the extent of testing are based on the availability of resources within the client's environment designated for testing. Any patches or changes to software or hardware are communicated to the personnel responsible for implementing the change. Any policy updates are documented in the appropriate document and noted in the change control log within the document. Critical patches are evaluated monthly by subject matter engineering groups in conjunction with the Information Security Manager. Changes are categorized and ranked according to standard or non-standard changes, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests.

WE'RE HERE TO HELP

D3 Security's proven incident management platform empowers security operations with a full-lifecycle remediation solution and a single tool to determine the root cause of and corrective action for any threat—be it cyber, physical, financial, IP or reputational.

D3 SECURITY

www.d3security.com

SALES CONTACT

1-800-608-0081 (Ext. 2)
sales@d3security.com

FOLLOW US