**Paradigm Software Technologies, Inc. DBA Nexelus Risk Assessment Report (RAR)**

**1. Introduction**

**1.1 Purpose**

The purpose of this risk assessment was to identify threats and vulnerabilities related to Paradigm Software Technologies, Inc. DBA Nexelus’s **Nexelus Application**. This risk assessment serves as the basis for identifying risk mitigation safeguards and procedures related to the system(s).

**1.2 Scope of Risk Assessment**

**Nexelus**

The scope of this risk assessment includes all components of the system(s), along with the implemented (or planned) safeguards to manage the vulnerabilities that could be exploited by internal or external threat events. If exploited, these vulnerabilities could result in:

* Unauthorized disclosure of data
* Unauthorized modifications to the systems and or their data
* Denial of service and/or access to data to authorized users

This Risk Assessment Report (RAR) evaluates the confidentiality (protection from unauthorized disclosure of system and data information), integrity (protection from improper modification of information), and availability (loss of system access) of the system(s). Recommended security safeguards will allow management to make decisions about security-related initiatives.

**1.3 Participants**

The following is a list of members involved in the company’s Risk Assessment process:

|  |  |
| --- | --- |
| **Role** | **Participant Name** |
| System Owner | Imran Rahman |
| Security Administrator | Tao Lin, Peter Platowski |
| Operations and Human Resource | Tauseef Shahzad |
| Product Owner | Asim Jameel |

**2. Risk Assessment Approach**

This initial risk assessment was conducted using a threat-based and vulnerability-oriented approach, and a qualitative/semi-quantitative methodology. Risks will be determined and assessed based on system vulnerabilities, mitigating factors already in place, threat events related to those vulnerabilities, the probability (likelihood) of those threats occurring, and the impact of those threats on the system vulnerabilities.

The identification of the company’s vulnerabilities and the threats against those vulnerabilities will be utilized continuously throughout the entire lifecycle of the organization in order to manage risk.

**2.1 Techniques Used**

|  |  |
| --- | --- |
| **Technique** | **Definition** |
| Risk Assessment Tool | The assessment team used the Drata software as a service platform to identify and assess applicable risks. |
| Assessment Tools | The assessment team used several security testing tools to review system configurations and identify vulnerabilities in the application. The tools included nmap, Rapid7 |
| Vulnerability Sources | The team accessed several vulnerability sources to help identify potential vulnerabilities. The sources consulted included:  • Microsoft Security Advisories ([www.microsoft.com/security](http://www.microsoft.com/security))   * Rapid 7 Vulnerability Report |

**2.2 Risk Model**

By identifying relevant threats and present vulnerabilities, risks associated with the aforementioned system(s) were selected and assessed using the Drata Risk Manager. Applicable risks were selected from the Risk Library and evaluated based on a simple risk model reflecting the relationship between threats and vulnerabilities:

**Risk = Likelihood x Impact**

Each component was defined and valued qualitatively and semi-quantitatively.

**2.2.1 Threat Likelihood**

The assigned likelihood value represents the probability of a threat event occurring. The higher the value, the greater the probability.

|  |  |
| --- | --- |
| **Likelihood Value** | **Likelihood Definition** |
| 1 | Once in 100+ years or less (<10% chance of occurrence over the life of the company) |
| 2 | Once in 50 to 100 years (10% to 35% chance of occurrence over the life of the company) |
| 3 | Once in 25 to 50 years (35% to 65% chance of occurrence over the life of the company) |
| 4 | Once in 2 to 25 years (65% to 90% chance of occurrence over the life of the company) |
| 5 | Up to once in 2 years or more (90% or greater chance of occurrence over the life of the company) |

**2.2.2 Magnitude of Impact**

The assigned impact value represents the assessed severity of a threat against a known vulnerability. The greater the value, the greater the impact.

|  |  |
| --- | --- |
| **Impact Value** | **Impact Definition** |
| 1 | • Minimal loss/damage • Local media attention quickly remedied • Not reportable to regulator • Isolated staff dissatisfaction |
| 2 | • Minor loss/damage • Local reputational damage • Reportable incident to regulator, no follow up • General staff morale problems and increase in turnover |
| 3 | • Moderate loss/damage • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Widespread staff morale problems and high turnover |
| 4 | • Significant loss/damage • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice |
| 5 | • Massive loss/damage • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Multiple senior leaders leave |

**2.2.3 Risk Score Matrix**

In representation of the aforementioned likelihood and impact scores, we utilized a risk matrix that can be used to analyze and prioritize risks. The risk ratings were calculated as follows:

|  |  |
| --- | --- |
| * **LOW:** | Less than or equal to 4.0 |
| * **MEDIUM:** | Greater than 4.0 but less than or equal to 9.0 |
| * **HIGH:** | Greater than 9.0 but less than or equal to 16.0 |
| * **CRITICAL:** | Greater than 16.0 |

If you have adjusted your risk scoring, you will need to manually insert your custom graph here for inclusion in the downloaded report

**3. System Characterization**

**3.1 System Components**

|  |  |
| --- | --- |
| **Component** | **Description** |
| Applications | .Net/.Net Core running under Microsoft Internet Information Server |
| Databases | Microsoft SQL Server |
| Operating Systems | Microsoft Windows |
| + | + |

**3.2 Physical Location(s)**

|  |  |
| --- | --- |
| **Location** | **Description** |
| Data Center | Hosted on Microsoft Azure |
| Help Desk | Hosted on Microsoft Azure |
| Network Operations Center | Hosted on Microsoft Azure |

**3.3 Data Used by System**

|  |  |
| --- | --- |
| **Data** | **Description** |
| Confidential Information | Client Data |
| PII Information | No PII information is stored in application |
| Financial Information | Accounts Payables, Sales |

**4. Risk Assessment Report Results from Drata**

|  |  |  |
| --- | --- | --- |
| **Role** | **Participant Name** | **Date of Completion** |
| System Owner | Imran Rahman | Date |
| SOC | Tauseef Shahzad |  |
| Peter Platowski | Network Administrator |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk**  **ID** | **Risk** | **Risk Category** | **Impact** | **Likelihood** | **Risk Score** |
| AC-02 | Login Credentials - Impersonation of an Authorized User | Access Control | 4 | 4 | 16 |
| AC-04 | Password Management - Password Cracking | Access Control | 3 | 4 | 12 |
| AA-02 | Continual Improvement - Adaptive Threat Behavior and Methods | Assessments & Audits | 5 | 2 | 10 |
| SD-03 | Software Development Standards - Insecure Coding | Software Development | 4 | 2 | 8 |
| PV-02 | User Access Rights - Disclosure of Sensitive Data | Privacy - Access | 4 | 2 | 8 |
| IN-32 | Primary Facility - Operational Disruption Due to Geopolitical Incident or War | Incidents - Environmental | 4 | 2 | 8 |
| AA-10 | Organizational Change Management - Operational Disruption | Assessments & Audits | 4 | 2 | 8 |
| GV-12 | Unreviewed Contracts - Data Access Disruption | Governance - Compliance/Legal | 4 | 2 | 8 |
| AC-01 | Improper Access Management - Accidental Escalation of User Privileges | Access Control | 3 | 2 | 6 |
| GV-26 | Communication System Management - Resource Contention | Governance - Planning | 3 | 2 | 6 |
| GV-30 | Lack of Oversight and Screening - Unqualified Employees | Governance - Policies | 5 | 1 | 5 |
| PH-08 | Support Infrastructure Security - Physical Attack | Physical - Site | 5 | 1 | 5 |
| IN-29 | Primary Facility - Operational Disruption Due to Earthquake | Incidents - Environmental | 5 | 1 | 5 |
| IN-10 | Essential Software, Firmware, or Hardware - Operational Compromise | Incidents - Breach, Compromise, UA Modification | 5 | 1 | 5 |
| AA-09 | Network Management - Advanced Persistent Threat | Assessments & Audits | 5 | 1 | 5 |
| AC-05 | User Authentication - Man-in-the-Middle Attack | Access Control | 5 | 1 | 5 |
| AM-07 | Personal Devices - Malware | Asset Management | 4 | 1 | 4 |
| SY-06 | IT Systems - Malware | Systems - Configurations | 4 | 1 | 4 |
| PV-01 | Third Party Access Control - Unauthorized Access | Privacy - Access | 4 | 1 | 4 |
| IN-37 | Backup Facility - Operational Disruption or Loss Due to Disaster | Incidents - Recovery & Remediation | 4 | 1 | 4 |
| IN-31 | Primary Facility - Operational Disruption Due to Flood | Incidents - Environmental | 4 | 1 | 4 |
| IN-25 | User Access Rights - Unauthorized Systems Modification | Incidents - Breach, Compromise, UA Modification | 4 | 1 | 4 |
| AA-01 | Activity Log Evaluation - Unauthorized System Access | Assessments & Audits | 4 | 1 | 4 |
| GV-25 | Business Impact Assessment or Continuity Planning - Operational Disruption | Governance - Planning | 4 | 1 | 4 |
| AM-01 | Asset Diversification - Operational Disruption | Asset Management | 4 | 1 | 4 |
| AM-10 | Unsecured Physical Storage - Theft | Asset Management | 4 | 1 | 4 |
| AC-03 | Login Credentials - Security Violations | Access Control | 3 | 1 | 3 |
| PV-36 | Indefinite Data Retention Without Purpose | Privacy - Storage Limitation | 3 | 1 | 3 |
| SY-01 | Common Business Software - Malware | Systems - Configurations | 3 | 1 | 3 |
| AA-04 | Critical System Dependencies - DoS | Assessments & Audits | 3 | 1 | 3 |
| AA-05 | Employee Awareness - Inconsistent or Unclear Risk Messaging | Assessments & Audits | 3 | 1 | 3 |
| AM-09 | Removable Media Devices - Malware | Asset Management | 3 | 1 | 3 |
| AA-07 | Exposure - Physical and Cyber Reconnaissance | Assessments & Audits | 3 | 1 | 3 |
| AA-08 | Exposure - Zero-day Attack | Assessments & Audits | 3 | 1 | 3 |
| IN-18 | Privacy Data Encryption - Password Compromise | Incidents - Breach, Compromise, UA Modification | 3 | 1 | 3 |
| IN-15 | Login Credentials - Unidentified Security Incidents or Breaches | Incidents - Breach, Compromise, UA Modification | 3 | 1 | 3 |
| IN-11 | Exposure - Data Channel Interception and Unauthorized Access/Modification | Incidents - Breach, Compromise, UA Modification | 3 | 1 | 3 |
| GV-31 | Outdated Policies and Procedures - Operational Disruption | Governance - Policies | 3 | 1 | 3 |
| PH-06 | Third Party Access Control - Tampered Sensitive Equipment | Physical - Access | 2 | 1 | 2 |
| PL-07 | Information System Access Control - Insider Threat | People - Personnel | 2 | 1 | 2 |
| AM-02 | Asset Lifecycle Management - Unreliable Equipment | Asset Management | 1 | 1 | 1 |
| SY-19 | Disk Error - Storage Corruption | Systems - Data Protection | 1 | 1 | 1 |

**5. Risk Treatment**

A risk treatment is built based on this RAR, and will be managed in Drata.