RFR Holdings, Inc.
InfoSec Policy and Procedures

Red Flag Reporting

Protecting Organizations and Their People

9/1/2019

The intent of this document is to provide guidelines and policies for information technology use to assure the safety of the company's information technology assets and employees.

Table of Contents

Identity and Password Management Policy

The purpose of this policy is to define required access control measures to all Company systems and applications to protect the privacy, security, and confidentiality of Company information technology resources and data.

1. Identity is the unique characteristics assigned to every individual or system to enable decisions about the levels of access that should be assigned.

1.1 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

1.2 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

1.3 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

1.4 You may access, use or share Company proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

2. Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to Company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.1 Password Creation

2.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

2.1.2 Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.

2.1.3 User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts

2.2 Password Change

2.2.1 Passwords should be changed only when there is reason to believe a password has been compromised.

2.2.2 Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

2.3 Password Protection

2.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Company information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

2.3.2 Passwords may be stored only in “password managers” authorized by the organization.

2.3.3 Do not use the "Remember Password" feature of applications (for example, web browsers).

2.3.4 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

2.4 Password Construction Guidelines. Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

2.4.1 Guidelines: Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 8 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include “It’s time for vacation” or “block-curious-sunny-leaves”. Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of “Welcome123” “Password123” “Changeme123

Principles of Authorization

1. Least Privilege

An authorization should only provide the privileges required for the function to be performed and no more. Following this principle helps ensure proper workflows are followed and access to functions that may expose data is contained as much as possible.

2. Separation of Duties

When an authorization is granted to an account it must be approved by multiple individuals. Multiple approvers ensures that the Principle of Least Privilege is followed from both a technical and process perspective, decreases opportunity for conflict of interest or fraud, and reduces the risk of error. As applied to authorization, separation of duties requires that the administrative and technical approver are not the same person, or if they must be, then the Data Custodian is not filling either role.

3. Roles in Authorization

Authorizing an account to use a system or application is responsibility of our IT department.

Secure Networks

Employees should only conduct Company business, access Company systems and data over secure networks. Employees should not connect Company devices to public WiFi or conduct business, access Company systems or data over public WiFi even on PCD, this includes checking Company Email Account.

1. Company network: at this time the Company does not own or manage a network as all employees work remotely and server/infrastructure is provided as part of our service agreement with Microsoft.

2. Remote workers are encouraged to use their home internet service and should either connect directly with an ethernet connection or through wireless connection.

2.1 Home WiFi networks should be secured using the following guidelines:

- Change your default router password. The default passwords of most routers include words and other strings that make them relatively easy to remember and type in but also easy for password-cracking software to break. Use strong passwords with a random mix of upper- and lowercase letters, numbers, and symbols.
- Change the default name of the router. The default name of most routers is the manufacturer and model of the router. Hackers can use this information to help them break in. Change the name of the router to conceal its make and model.
- Hide the router. Have you noticed that when you open your laptop or turn on your phone at Starbucks or the airport you see a list of Wi-Fi connections which are in range that you might potentially join? You can make a change to your router so that it does not appear in such broadcasts. Then the only way to find it will be to type in its name. For instructions on how to hide your router, see the manual.
- Turn off remote management. You'll most likely never have any need for this, and it's a potential opening to hackers. It's best to shut it off.
- Change the default administrator password. There are only a few of these in standard use and the hackers know what they are. Change yours. See your router's manual for instructions.
- Stay logged OFF as an administrator. You don't need this functionality and the hackers can exploit it. Turn it off and keep it off.

- Change the settings to allow access only by MAC address. MAC means Media Access Control address, and every device that can connect to the Internet has a unique one. If you change your router to allow access only by MAC address, then the only devices which can connect to it are the MAC addresses you've told it to accept.

Server Security

Red Flag Reporting maintains all servers exclusively within the Microsoft Azure environment, primarily as services. Servers are managed by Microsoft Technical Support under agreement in accordance to latest Microsoft Azure InfoSec policies and Microsoft Operational Security Assurance (OSA).

Application Security

Application development and the security of the development life cycle is performed by Microsoft engineers on behalf of Red Flag Reporting governed by latest Best Practices for Secure Development published by Microsoft.

1. Logical security

Our solution is built with application security roles and controls. We help secure the service infrastructure with multi-tier administration, server monitoring, access control, and security standards and policies. Microsoft provides a team to ensure service reliability and continuity with standardized operations, defined change and incident management, and ongoing investments in hardening our defenses.

Data Center Security

Microsoft Corporation provides Red Flag Reporting a cloud services environment that features vigorous security and continuous access to applications and data. This service ensures increased security at each phase of the cloud services delivery model and for every user interaction—physical datacenter, network connectivity, service hosting platform, and user and administrator access—to help you reap the demonstrated benefits of cloud services while minimizing your overall risk.

Ours is a security-hardened solution that has been designed using the principles of the Microsoft Security Development Lifecycle. Security roles allow us to further secure data by controlling user access through a set of access rights and permissions.

1. Physical security

   Microsoft datacenters provide 24-hour monitoring through physical controls, video surveillance, and access control to ensure only authorized personnel can manage applications and services.

Features we require Microsoft maintain:

- **Redundant power supplies.** To ensure business continuity, when power is lost, there are two power supplies for each datacenter: a battery provides short-term power until diesel generators can kick in. Microsoft has contracts with multiple fuel suppliers to ensure fuel delivery for the generators when it is needed.
- **Natural disaster control.** Microsoft provides seismically braced racks where required and fire prevention and extinguishing systems to protect datacenters against natural disasters.
- **Physical monitoring.** Microsoft strengthens physical security with motion sensors, 24-hour secured access, video camera surveillance, and security breach alarms.
- **Distributed Microsoft datacenter locations:** Our solution is deployed in Microsoft datacenters that are located in disperse geographies (currently only US based datacenters).
- **Secure network design and operations:** Each Microsoft datacenter provides multiple separate network segments. Segmentation helps ensure physical separation of critical, back-end servers and storage devices from the public-facing interfaces.
- **Redundant Network**: A redundant network provides full failover capability and helps ensure 99.9 percent network availability.
- **Anti-Virus**: Anti-viral and anti-intrusion measures further secure data.
- **Secure Access for Support:** All remote connections by Microsoft operations personnel must be made via Remote Desktop Service and two-factor authentication.

Incident Management

Each system custodian must develop and review at least annually a system-level incident response plan that contains:

- Names and contact information for the incident response team, including:
    - Security Contact and alternate contact(s) who have system admin credentials, technical knowledge of the system, and knowledge of the location of the incident response plan.
- System details, or reference to the location of such information, including:
    - Data Flow Diagrams
    - Network Diagrams
    - Logging information
- Procedures for reporting and handling a suspected incident, defined per role: Sys Admin, Bulk Access User, End User, e.g.,
    - Who to contact

1. **What is a Security Incident?**

A security incident in the context of this requirement is an event that compromises or has the potential to compromise:

- the operation of covered core systems or
- confidentiality or integrity of covered data assets

1.1 A security incident may involve any or all of the following:

- a violation of organization computer security policies and standards
- unauthorized computer or data access
- presence of a malicious application, such as a virus
- presence of unexpected/unusual programs
- a denial of service condition against data, network or computer
- misuse of service, systems or information
- physical or logical damage to systems
- computer theft