

# **Red Barons Acceptable Use Policy:**

## **1. Purpose:**

The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at Red Barons. These rules are in place to protect the employee and the organization. Inappropriate use exposes organizational assets to cyber risks including virus attacks including ransomware, compromise of network systems and services, data breach, and legal issues.

## **2. Scope:**

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by Red Barons, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers of Red Barons and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with organizational policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Red Barons, including all personnel affiliated with third parties. This policy also applies to all equipment that is owned or leased by Red Barons.

## **3. Policy:**

### **3.1 General Use and Ownership**

- 3.1.1 Any proprietary information stored on electronic and computing devices whether owned or leased by Red Barons, the employee or a third party, remains the sole property of Red Barons. You must ensure through legal or technical means that proprietary information is protected in accordance with all applicable policies, standards, regulations, and laws.
- 3.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of organizational proprietary information.
- 3.1.3 You may access, use or share Red Barons' proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- 3.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- 3.1.5 For security and network maintenance purposes, authorized individuals within Red Barons may monitor equipment, systems, and network traffic at any time, per organizational auditing policies.
- 3.1.6 Red Barons reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### **3.2 Security and Proprietary Information**

- 3.2.1 All mobile and computing devices that connect to the internal network must comply with all applicable policies, standards, regulations, and laws.
- 3.2.2 System level and user level passwords must comply with organizational password policies. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- 3.2.3 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- 3.2.4 Postings by employees from a Red Barons email address to newsgroups or other online platforms are prohibited unless a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Red Barons is included.
- 3.2.5 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

### **3.3 Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Red Barons authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing company-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

### **3.3.1 System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Red Barons.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Red Barons or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting Red Barons business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
6. Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a company-owned computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Red Barons account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the Red Barons network.
15. Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Red Barons employees to outside parties.

### **3.3.2 Email and Communication Activities**

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that “the opinions expressed are my own and not necessarily those of the company”. Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies.
5. Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type.
6. Use of unsolicited email originating from within Red Barons’ networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Red Barons or connected via Red Barons’ network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

### **3.3.3 Blogging and Social Media**

1. Blogging or posting to social media platforms by employees, whether using company-owned property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of company-owned systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate organizational policies, is not detrimental to Red Barons’ best interests, and does not interfere with an employee’s regular work duties. Blogging or other online posting from company-owned systems is also subject to monitoring.
2. Employees are prohibited from revealing any information that is confidential or proprietary, trade secrets or any other material covered by organizational policies, standards, and federal regulations when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Red Barons and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in conduct prohibited by applicable policies, standards, regulations, and laws.
4. Employees may also not attribute personal statements, opinions or beliefs to Red Barons when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Red Barons. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, organizational trademarks, logos and any other Red Barons’ intellectual property may also not be used in connection with any blogging or social media activity

## **4. Policy Compliance:**

#### 4.1 Compliance Measurement

The IT Management department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

#### 4.2 Exceptions

Any exception to the policy must be approved by the IT Management team in advance.

#### 4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

### 5. **Related Standards, Policies and Processes:**

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

### 6. **Authorship/Revision History:**

12/18/2023 – “Acceptable Use Policy” created by David Renteria