# <Company Name> Cybersecurity Policy

| | |
|---|---|
| **Policy:** Cybersecurity Policy | **Table of Contents** |
| **Compliers:** Employees, Contractors, Stakeholders |  |
| **Effective Date:** Feb 21, 2024 | |

| | |
|---|---|
| **1 Purpose** | <Org name> is committed to ensuring the security and integrity of the data stored for athletes and coaches. This cybersecurity policy frames the actions set up to safeguard this exceptionally private information and the frameworks that house it. It focuses on operational practices for the protection of all information, data, files, and processing resources owned by <Org. name> |
| **2 Scope** | This policy applies to all employees, contractors, third-party partners, and stakeholders managing and accessing our data and systems. |
| **3 Statement of Policy** | **3.1 Password**<br><br>**3.1.1** Password should be 8-12 characters long and contain a combination of uppercase letters, lowercase letters, numbers, and special characters. Do not use name, user ID, date of birth, or contact numbers, company name, or any such common passwords to avoid easy guesses.<br><br>**3.1.2** Do not write passwords on paper or sticky notes.<br><br>**3.1.3** Password should be updated every 90 days. Reuse of the last 5 passwords is restricted. Reminders will be sent through email or pop-ups a week before. Failure to do so, the account will be temporarily suspended, and you need to contact the IT Support team.<br><br>**3.1.4** Passwords stored in the database should be encrypted and securely transmitted through different channels.<br><br>**3.1.5** Multi-factor Authentication (MFA) should be enabled to avoid unauthorized access.<br><br>**3.2 Email**<br><br>**3.2.1** Email must be secure using a strong password as mentioned in section 3.1. |

**3.2.2** Sending and receiving emails from personal email accounts is restricted. Company-provided email accounts must be used for work-related communications. Personal email accounts are not permitted for official correspondence.

**3.2.3** Beware of phishing emails that attempt to trick you by sending malicious attachments. Do not download any attachment that looks suspicious or from any unknown sender. Look for signs of phishing, such as misspelled email addresses, urgent requests for personal information, or suspicious links. Report any suspicious email to the IT department immediately as it could compromise security measures.

**3.2.4** Always recheck information before sending any email, for instance, the sender's name or email to avoid sharing sensitive data with unauthorized users.

### 3.3 Handling Sensitive Data and Removable Devices

**3.3.1** Sensitive data i.e. information related to users and employees must be locked in a storage room in physical offices. No unauthorized user should be allowed to access the information.

**3.3.2** Information must directly be filled in the database or system software instead of sticky notes or any paper. In the case of paper use, it should be discarded as soon as possible via a paper shredder.

**3.3.3** Use of external hardware devices, for instance, USBs, disks, Bluetooth, speakers, and so on are prohibited.

**3.3.4** Forwarding email from work email to personal email is restricted.

**3.3.5** Do not connect malware-infected USBs to systems to prevent the spread of any virus.

### 3.4 Locking Computers and Devices

**3.4.1** Devices must never be left unattended. Always log off or lock your screen before stepping away from your device.

**3.4.2** Systems must be password-protected with multi-factor authentication to protect against unauthorized access.

**3.4.3** Systems must be shut down after the shift will be ended.

### 3.5 Handling of Technology, Social Media, and Internet Access Standards

**3.5.1** Use of personal laptops, mobile phones, and other devices is restricted during working hours except break times. Smartphones should be either turned off or remain silent.

**3.5.2** Usage of workplace computers for personal use is strictly prohibited.

**3.5.3** Regular updates will be sent for installation of the latest software versions and anti-viruses.

| | |
|---|---|
| | **3.5.4** Usage of social media and other entertainment websites for example YouTube, Twitter, Facebook, Instagram, and so on is allowed in break time only on personal devices.<br><br>**3.6 Managing Incidents**<br><br>**3.6.1** In case of clicking on any suspicious link or from an unauthorized sender, report to the IT Support team on the same day.<br><br>**3.6.2** Report to the manager of your team in case of sharing any information or forwarding any email to unauthorized users of the organization. |
| **4 Responsibilities** | • The IT Support team will forward concerns or requests to the designated teams or persons.<br>• The software development team will be responsible for keeping track of all updated software, and installations or managing computer systems.<br>• The Information Security team will be responsible for logging, monitoring, managing and mitigating any cyber threats, phishing emails, or any cyber-attacks in response time. |
| **5 Verification of policy compliance** | • Regular audits will be conducted to verify the compliance of all the policies.<br>• Team leaders or managers will be responsible for checking or conducting audits for their team members in every 2 weeks. |
| **6 Penalties for non-compliance** | All employees, and users are meant to follow the above-mentioned policies, failure to implement those can result in termination in the following three stages.<br><br>• Verbal warning will be given as 1st warning.<br>• Written notice will be given in 2nd warning.<br>• Termination will be given as 3rd warning. |
| **7 References** | 1. "Creating an Effective Cloud Security Policy: Guide and Template", www.netwrix.com, https://www.netwrix.com/cloud-security-policy.html<br><br>2. "Company cyber security policy template", www.resources.workable.com, https://resources.workable.com/cyber-security-policy<br><br>3. "How to create a cloud security policy, step by step", www.techtarget.com, https://www.techtarget.com/searchsecurity/tip/How-to-create-a-cloud-security-policy-step-by-step |