Cyber Security Policy

1. Purpose

The purpose of this Cyber Security Policy is to outline the guidelines and responsibilities for safeguarding the data, systems, and technology infrastructure of Shockout.
As we increasingly rely on digital technology to collect, store, and manage information, we also face greater risks of cyber threats, human error, and system vulnerabilities.
This policy establishes measures to prevent, detect, and respond to potential security incidents and to promote a culture of vigilance across the organisation.

2. Scope

This policy applies to all employees, students, contractors, volunteers, and any other individuals who have temporary or permanent access to Shockout's digital systems, data, or hardware.

3. Policy Overview

Shockout is committed to maintaining the confidentiality, integrity, and availability of all digital information.
All members of the organisation share responsibility for protecting data from unauthorized access, disclosure, alteration, or destruction.

Key areas covered by this policy include:

- Confidential data protection
- Device and email security
- Password management
- Secure data transfer
- Incident reporting and response
- Remote work security
- Disciplinary procedures for breaches

4. Confidential Data

Confidential data is considered private, sensitive, and valuable. Examples include:

- Unpublished financial information
- Data relating to customers, students, partners, or vendors
- Course materials (e.g., choreography, module content)
- Student lists (current and prospective)

All individuals must protect confidential data in accordance with this policy and follow the instructions provided to avoid security breaches.

5. Device Security

When accessing company emails, systems, or files via digital devices (company-issued or personal), users must take the following precautions:

- Keep all devices password protected.
- Install and regularly update approved antivirus software (e.g., McAfee).
- Do not leave devices unattended or exposed.
- Install browser and system updates promptly.
- Access company systems only via secure, private networks.
- Never use another person’s device to access company accounts or lend devices to others.

Setup for New Devices

New employees receiving company-issued or personal laptops must:

- Set up strong password management systems.
- Install McAfee Anti-Virus software.
- Seek support from Human Resources (HR) or Facilities if unsure about setup or security configurations.

6. Email Security

Emails are a common entry point for phishing, scams, and malware. To mitigate these risks, employees and students should:

- Avoid opening unexpected attachments or clicking unverified links.
- Be cautious of “clickbait” or suspicious subject lines.
- Verify sender details and watch for signs of fraud (e.g., spelling errors, excessive punctuation, generic greetings).

If uncertain about an email’s legitimacy:

- Employees should contact the HR or Facilities Manager.
- Students should contact Student Support.

7. Password Management

Passwords are critical to system security. All users must:

- Use strong passwords (minimum 8 characters, including upper/lowercase letters, numbers, and symbols).
- Avoid using easily guessed information (e.g., birthdays).

- Keep passwords private and secure; destroy written copies once no longer needed.
- Update passwords every three months.

Users are encouraged to use secure password management tools (e.g., keychain systems).
If passwords are forgotten, temporary ones will be issued to allow users to reset them safely.

8. Secure Data Transfer

When transferring data:

- Only share sensitive or confidential information when necessary.
- Use company-approved systems or networks; never public Wi-Fi.
- Confirm that recipients are authorised and have appropriate security measures.
- Report any suspected scams, breaches, or hacking attempts immediately.

The Business Operations, HR, or Facilities teams are responsible for investigating incidents and issuing alerts if necessary.

9. Reporting and Response

Employees must report perceived attacks, phishing attempts, or malware immediately to Business Operations, HR, or Facilities.
These teams will:

- Investigate incidents promptly.
- Take corrective measures to contain and resolve breaches.
- Communicate company-wide alerts if broader risks are identified.
- Provide guidance on identifying and preventing scams.

10. Additional Security Measures

To strengthen security across the organisation, employees must:

- Lock or turn off screens when leaving desks.
- Report lost, stolen, or damaged devices immediately.
- Change all passwords if a device is stolen.
- Refrain from downloading unauthorised or illegal software.
- Avoid visiting suspicious or unsafe websites.

Shockout's Business Operations, HR, and Facilities teams will:

- Provide antivirus software, firewalls, and access authentication systems.
- Offer security training and updates on new threats.
- Investigate all security incidents thoroughly.

11. Remote Work

Remote employees must follow all provisions of this policy.
They must:

- Use encrypted connections and secure networks.
- Follow data protection standards when accessing company systems remotely.
- Contact Business Operations, HR, or Facilities for support if needed.

12. Disciplinary Action

All individuals are expected to comply with this policy.
Failure to do so may result in disciplinary action as follows:

Type of Breach	Action
Minor or unintentional breach	Verbal warning and mandatory retraining
Repeated or significant breach	Written warning or suspension
Intentional or large-scale breach causing damage	Termination and potential legal action

Each case will be reviewed individually.
Repeated disregard for cyber security instructions may also lead to disciplinary measures, even if no actual breach occurs.

13. Commitment to Security

Shockout is dedicated to ensuring that all students, employees, partners, and customers feel confident that their data is safe.
Cyber security is a shared responsibility — through vigilance, awareness, and compliance, we can maintain trust and protect our digital environment.