Staffroom Software – Security Policy

(Version: 1.0)

1. **Introduction**

   There is no such thing as “perfect security”. We have to compromise between increased levels of security and the convenience to you in transacting with us.

2. **Our security responsibilities**

   We will ensure that:

   - We host our website in a secure server environment that uses a firewall and other advanced security measures to prevent interference or access from outside intruders.
   - The information you give to us that is stored on or passes through our systems is protected. Encryption is used to protect the personal information you give us. This includes using your credit card on our website (see below).
   - The links from our systems to systems under the control of third parties (for example our payment gateway) are secure.
   - We perform regular backups of data to ensure it can be recovered in the case of a disaster.
   - We log all access to our system. If any unauthorised behaviour should occur, this will assist us in identifying and resolving the issue.
   - We take reasonable steps to secure your payment information and use a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of the transaction concerned.

3. **Our security disclaimers**

   Please note the following:

   - The third parties whose systems we link to are responsible for the security of information while it is collected by, stored on, or passing through the systems under their control.
   - We will use all reasonable endeavours to ensure that our website and your information is not compromised. However, we cannot guarantee that no harmful code will enter our website (for example viruses, bugs, trojan horses, spyware or adware). You should be aware of the risks associated with using websites (addressed below).
   - If you experience a problem or loss that is caused by information you provided to us, your computer being compromised in some way or by something beyond our control, we cannot take responsibility for causing the problem. We will, however, do our best to help you if we can.

4. **Your security responsibilities**

4.1 ***Recommended steps***. You should:

   - Install and activate appropriate security software on your computer. This should include anti-virus, anti-spyware and anti-spam software.
   - Run regular scans of your computer for viruses.
   - Update your security software to ensure you are always running the current version.

4.2 ***Additional steps***. Other steps you should take to help protect your computer include:

   - Check your Internet browser’s security settings for ways to make your browsing more secure.
   - Make sure that you have entered secure pages when filling in your credit card details. Look for a small yellow lock commonly seen at the bottom right of your browser and http changes to https on the address bar.
   - Sign out after you have transacted electronically.

5. **Protecting your password**

   You should:

   - Never share your password with anyone.
   - Never send your password via email.
   - Make your password as strong as possible.

6. **Phishing**

6.1 ***Secure URL***. You must only log in to your account from a page that has a web address ending in mystaffroom.net or intouch.zone.

6.2 ***No confirmation through links***. We will never ask you to confirm your username and password or other sensitive information by clicking on any links in an email other than the email link we send you at registration to verify your email address. Be aware of “phishing” attacks where criminals attempt to obtain your sensitive information by sending you an email, masquerading as an email from us, asking you to access your account or verify information via links in the email, or diverting you to a fake website. Please report any suspected phishing attacks to us immediately to prevent any harm to you or other users.

7. **Contact us**

   You must report any suspicious or unauthorised activity relating to your use of our website by contacting us. This will help make our website as secure as we can.

8. **Our right to take action**

   We reserve the right to take whatever action we may deem necessary at any time to preserve the security and reliable operation of our system. You undertake not do (or permit anything to be done) that may compromise the system under our control.