Digital Security Checklist

Are you looking to enhance your digital security?

By following this checklist, your team of recruiters and hiring managers can help ensure that your recruitment process is secure and that sensitive information is protected.

Security Must-Haves

- [ ] **Educate employees on digital security:** Provide regular training and education on digital security best practices to ensure that all employees understand the importance of digital security.
- [ ] **Conduct regular security audits:** Regularly audit your security protocols and procedures to ensure that they are up to date and effective.
- [ ] **Create a password policy:** Ensure that all employees use strong passwords that are difficult to guess. Passwords should include a combination of upper and lower case letters, numbers, and special characters. Passwords should also be changed regularly.
- [ ] **Implement two-factor authentication:** This extra layer of security can help prevent unauthorised access to sensitive data. Two-factor authentication requires the user to enter a code or token in addition to their password.
- [ ] **Use encryption:** Sensitive data such as personal information or financial details should be encrypted to prevent unauthorised access. Encryption ensures that only authorised personnel can access the data.
- [ ] **Use secure file sharing:** Ensure that sensitive documents are not sent via unsecured channels such as email. Instead, use a secure file sharing service that requires a password or secure link to access the files.
- [ ] **Implement antivirus and firewall protection:** Install antivirus software and firewalls on all computers and servers to protect against malware and other cyber threats.
- [ ] **Regularly back up data:** Ensure that all data is regularly backed up and stored securely in case of a data breach or loss.

Recruitive info@recruitive.com 0345 60 00 550