CYBERSECURITY CHECKLIST FOR CONVEYANCING FIRMS

01. Implement strong password policies

- Require complex passwords of 12+ characters, including uppercase and lowercase letters, numbers, and symbols.
- Avoid using common words, personal information, or passwords identical to those used for other accounts.
- Mandate regular password updates.

02. Enable Two-Factor Authentication (2FA)

- Activate 2FA for all accounts, prioritising those with access to sensitive data.
- Ensure users are familiar with the 2FA setup process.

03. Train your team against cyber threats

- Train staff to recognise phishing attempts and other cyber threats.
- Schedule regular cybersecurity awareness sessions to update employees on emerging threats.

04. Secure your network

- Protect your systems with firewalls, VPNs, and encryption.
- Restrict network access based on user roles and responsibilities.

05. Back up data regularly

- Set up automated backups and store them in secure, off-site locations.
- Periodically test your backup restoration process to ensure data can be retrieved when needed.

06. Monitor & audit

- Continuously monitor network traffic for unusual activity.
- Conduct regular audits of cybersecurity practices to identify vulnerabilities.

07. Limit data access

- Grant access to sensitive data based strictly on user roles.
- Regularly review and update user access permissions to reflect role changes or staff departures.
- Do not share accounts or passwords.

triSearch®