LAW SOCIETY
OF SOUTH AFRICA

ICT minimum security policy for cyber breaches

Insurers may repudiate cybertheft claims if minimum standard security policies are not in place. Practitioners are advised to read their policies carefully and implement the minimum-security standards that are included in the policy.

Below is what some insurers require as minimum ICT security policies:

- To implement firewalls to restrict access to digitally stored sensitive information.
- To ensure anti-virus and anti-malware software implemented on all desktops, laptops and sensitive systems (where applicable and in accordance with best practice recommendations) and kept up to date as per the software providers' recommendations.
- It is suggested that all security updates are set to automatically update the last security patches and updates on all sensitive system.
- Mobile devices that can link to sensitive systems should have similar updates and charging of phones in public access, should have a "USB condom" that prevents hacking or virus attacks via the charging port.

Password controls implemented on sensitive systems. These controls must include:

- Password length of at least 8 (eight) characters.
- User account passwords to be changed at least every month.
- Security policies must be strictly applied and monitored as the common vulnerability is via staff apathy, "thus requiring ongoing engagement, awareness campaigns and training of employees in security protocols, including phishing etc, employees can become the part of the defence."
- Passwords configured which are not common dictionary words and cannot within reason be deemed widely used or easily guessable e.g. date of birth, 1234, password etc.
- Special characters must be included in password and randomly selected.

- User accounts configured to lockout as a result of at most 10 failed authentication attempts.
- All default installation and administration accounts secured via changing the account password and where possible disabling, deleting or renaming the account.
- Administrative and remote access interfaces such as Remote Desktop Protocol (RDP) are not accessible via the open internet. Where such interfaces are required these are accessible exclusively over secured channels such as Virtual Private Network (VPN) connections.
- Controls implemented to restrict wireless network access to sensitive systems and sensitive information to authorised users only.

Controls to include at least:

- enabling encryption of wireless network traffic;
- changing default access passwords to complex passwords comprising lowercase letters, uppercase letters, numbers, special characters and symbols;
- implementing authentication to access the wireless network; and where possible restricting wireless network access to known devices.

- Controls implemented to restrict physical access to offices, server rooms/sensitive processing facilities and if applicable remote locations including disaster recovery sites to authorised users.
- The system and/or activity logs for all sensitive systems should be stored for a minimum period of 6 (six) months.
- User privileges for users with access to sensitive systems and sensitive information must be revoked immediately upon termination of employment.

Other polices that are required:

- Documented disaster recovery and business continuity plans.
- Backups at least weekly and stored offsite or on cloud servers.
- Monitor and ensure the successful generation of backups.
- Stress test to be conducted on security including the ability to restore data from backups at least biannually.