

Technology Standards

These Technology Standards (the “Technology Standards”) constitute the Technology Standards as defined in the license agreement (the “Agreement”) entered into between Wasatch Front Regional Multiple Listing Services, Inc. (“WFR”) and the applicable vendor (the “Vendor”). Terms not otherwise defined in these Technology Standards shall have the meaning set forth in the Agreement. Vendor shall use at least, and without limitation, the following security protection in connection with use, access, and display of Licensed Listings:

Physical Security

- The security perimeter is clearly defined and the facilities physically sound.
- The walls are of solid construction.
- External doors protect against unauthorized access.
- Access rights to secure areas are regularly reviewed and updated.
- Access rights to secure areas are changed when personnel changes.
- Key storage is physically protected.
- Media containing sensitive information is protected against unauthorized access.
- Procedures are in place to handle secure disposal of backup media and other media containing sensitive information.

Remote Access

- Only users with a specific business requirement are granted remote access capabilities.
- Users are authenticated prior to accessing corporate network resources.
- Authentication is in the form of a unique username and password.
- Secure encrypted communications are used for remote administration of production systems and applications.
- Remote administration protocols, such as SSH, Telnet, PC Anywhere, Windows Terminal Server, or Remote Desktop, limit access to only trusted networks using a firewall.

Network Access

- Access control devices such as a firewall are used to separate public, 3rd party, and corporate networks.
- Users are located on separate network segments from those containing servers.
- Users’ segments are separated from server segments by a firewall or equivalent access control device.
- Network access policies disallow all access by default.
- Access policies are audited to identify out dated policy rules.
- Access control measures include username and password authentication.
- User access is restricted on a need-to-know basis.
- Maintenance accounts and remote support access are disabled if they are not required.

- Privileged and administrative accounts are strictly controlled.
- Vendor default security settings are changed on production systems before the system goes into production.
- Production systems are hardened by removing all unnecessary tools installed by the default configuration.
- All production systems are updated with the latest security related patches released by the vendors of various components.
- The router configuration is secured.
- Egress and ingress filters are installed on all border routers to prevent impersonation with spoofed IP addresses.
- If routers and other network devices are configured remotely, a secure communication protocol is used to protect the communication channel from eavesdropping.
- Routers are configured to drop any unauthorized packets.
- Routers are configured to prevent remote probing.
- Changes to the firewall need authorization.
- The network segment containing the servers for the Web presence are separated from the Internet with a firewall.
- The network segment containing the servers for the Web presence are separated from the network segment containing the internal servers with a firewall.
- All Internet accessible hosts (for example, firewall, Web server, router, etc.) are periodically updated and patched for security vulnerabilities.

System Security

- Vendor-supplied defaults are changed before a system is placed into production.
- Standard builds for each system class exist.
- Server builds take into account all known security vulnerabilities and industry best practices.
- Systems are configured to only run necessary services.
- Vendor-supplied security patches are installed within one month of release.
- A process exists to identify newly discovered security vulnerabilities applicable to the environment.

Privileged Account Management

- When an employee leaves the company, the account and password are immediately revoked.
- Privileged accounts have an individual username and password that is not shared.
- Accounts are reviewed on a yearly basis to ensure that out-of-date or unknown accounts do not exist.
- Unique username and passwords are used to authenticate.
- Security management controls the addition, deletion, and modification of IDs.
- Information security management (a) does not permit group passwords, (b) requires the minimum length of at least 7 character passwords, (c) requires passwords not be found in any commonly used dictionary, and (d) requires password choice to contain at least 1 number or 1 symbol.