Future Technologies – Remote Access Policy

Purpose:

The purpose of this policy is to define the standards, procedures, and restrictions for Future Technologies when connecting remotely to residential customers' computers to provide technical assistance.

Scope:

This policy applies to all employees, contractors, vendors, and agents of Future Technologies who access residential customers' systems and networks remotely for support purposes.

1. Policy

1.1. Authorization:

- Remote access to a customer's computer must be authorized by the customer.
- Access privileges must be limited to what is necessary to provide the requested support.

1.2. Customer Consent:

- Explicit consent must be obtained from the customer before initiating a remote access session.
- Customers must be informed of the purpose and scope of the remote access session.

1.3. Authentication:

- Secure methods must be used for remote access, including tools like ScreenConnect.
- Authentication should be handled securely, ensuring that access credentials are protected.

1.4. Secure Connection:

- All remote connections must use secure protocols to ensure data encryption during transmission.
- Public Wi-Fi should be avoided by Future Technologies' employees when accessing customers' systems. If necessary, a VPN must be used.

1.5. Device Security:

- Only company-approved devices may be used by Future Technologies for remote access. These devices must comply with the company's security standards.
- Anti-virus and anti-malware software must be installed and regularly updated on all devices used for remote access.
- Devices must have the latest security patches and updates installed.

1.6. Data Protection:

- No customer data should be downloaded or stored on Future Technologies' devices without explicit customer consent.
- Remote access sessions must be terminated as soon as the assistance is complete.
- Data encryption must be used for any sensitive information shared during the remote session.

1.7. Monitoring and Logging:

- All remote access activities must be logged and monitored. Logs should be reviewed regularly for unauthorized access or unusual activities.
- Any suspicious activities or security incidents must be reported to the customer immediately.

1.8. Compliance:

- Remote access must comply with all applicable laws, regulations, and company policies.
- Regular audits and reviews must be conducted to ensure compliance with this policy.

2. Review and Revision

This policy will be reviewed annually and updated as necessary to ensure it remains current and effective.