Le-Ru Telephone Company

CPNI and Red Flag Policy

General Information on CPNI

CPNI History

In the Telecommunications Act, section 222, the FCC identifies the need for Privacy of Customer Information. It states that every telecommunications carrier has a duty to protect the confidentiality of customers' proprietary network information (CPNI). The original rules went into effect in 1998. In late 2005, the media reported that data brokers were advertising the ability to sell records of telephone subscribers calling patterns for marketing purposes. In April 2007, the FCC released Order 07-22 to strengthen its privacy rules in light of all of the identity theft issues throughout the United States.

Some of the new requirements include:

- Authentication requirements for call and non-call detail information
- Notices in writing to customers of account changes
- Notice of unauthorized disclosure of CPNI
- Annual CPNI certification to be filed with the FCC
- Opt-in approval for joint venture partner or independent contractors

What is CPNI?

It is information that a customer has made available to the carrier solely by virtue of the carrier-customer relationship. CPNI includes the quantity, technical configuration, destination, type, location, and amount of use a telecommunications service subscribed to by an individual customer. CPNI includes sensitive personal information, types of service purchased, phone numbers called, time/date/duration of calls, calling patterns, type of network, and the dollar amount the customer spends on services.

Acceptable Uses of CPNI:

- Exchange of customer information for the purpose of inter-carrier billing
- Marketing of services within the existing customer relationship
- Mass marketing (bill insert, direct mail, newsletters, etc) to ALL customers
- Installation/repair of services by independent contractors

What is Not CPNI?

- Subscriber lists for publication in a directory
- Subscriber information when made available for providers of emergency services when solely for the purpose of delivering/assisting in the delivery of emergency services
- Collective data that relates to a group/category of services or customers from which individual identities/characteristics have been removed

Opt-Out

Le-Ru Telephone Company must notify customers of their right to be excluded from marketing efforts for products and services outside the existing customer relationship. This is called "opting out". Le-Ru will send Opt-Out notices if the marketing of products/services are outside the existing customer relationship or if verbal sales/marketing efforts are made during a live customer interaction/exchange.

There are several ways to allow a customer to Opt-Out:

- Mail an Opt-Out form to the address of record and ask the customer to sign/return if they do not wish to receive marketing materials outside of the existing customer relationship
- This form can also be sent by fax, email, or bill insert

Special Email Requirements:

- Customer must pre-approve receiving Opt-Out notices via email
- The subject line must clearly identify its purpose
- Customer must be able to reply directly to disapprove and Opt-Out
- Le-Ru must re-issue by alternative means email notices that are returned as undeliverable and restart the 32-day count

Format Requirements from the FCC:

- Easy to read type and language
- Easily discernible packaging
- Full translation—if it is translated into any other language (not just a synopsis)
- Identify the purpose for which CPNI will be used

IMPORTANT NOTICE
FOR ALL LE-RU TELEPHONE COMPANY CUSTOMERS
PLEASE READ CAREFULLY

Federal law allows you, the consumer, to choose how we here at Le-Ru Telephone Company handle your Customer Proprietary Network Information (CPNI). CPNI is data that is not publicly available, such as the type of service you subscribe to, the number of telephone lines you have, and how much you use your services.

The federal law is designed to protect you, while allowing Le-Ru Telephone Co. to meet your communications needs. Le-Ru Telephone Co. values our customers and meeting your communication requirements, while protecting your privacy, is our main concern.

In order to meet the needs of our customers, we may share CPNI information with other companies, including our affiliate: Le-Ru Long Distance Company. We will only disclose your CPNI records for the specific intent to analyze and/or provide products or services. This allows us greater ability to tailor the services we provide to you.

Only Le-Ru Telephone Co. will use your CPNI. We will not share, sell, rent or otherwise disclose your CPNI to anyone else, including other companies.

You have the right, under federal law, to control how your CPNI records are used. Le-Ru Telephone Co. has the responsibility to protect your CPNI records. To restrict the use of your CPNI records for marketing purposes, you should complete the attached form.

STEP 1: Opt-Out Authorization complete the enclosed Customer Information Authorization Form and send it to the address below or email us at info@leru.net within 30 days of receiving this notice. You always retain the right to restrict the use of your CPNI. Restriction of the use of your CPNI records will remain valid until you contact us in writing or for two years, whichever comes first.

If you decide not to let us use your CPNI records, this will not affect, in any manner, the services to which you subscribe. Regardless of your decision, we will provide another notice about your rights in two years.

STEP 2: The new federal rules also limit the customer information that Le-Ru Telephone Co. can provide customers over the telephone. Le-Ru Telephone Co. is required to establish a password procedure to further protect our customer's CPNI. To establish a password, please complete Section 2: Customer Account of the form. Under federal regulations, Le-Ru Telephone Co. can only discuss customer information with the customer of record and/or authorized persons listed on the account. If you wish to add authorized persons to your account, please complete Section 3: Authorized Persons.

We thank you for your time and attention to this important matter.

Le-Ru Telephone Company
P.O. Box 147; 555 Carter St.
Stella, MO 64867
417-628-3844

CUSTOMER INFORMATION AUTHORIZATION FORM (2017)

CUSTOMER NAME _____

TELEPHONE # _____ ADDRESS _____

CITY _____ STATE _____ ZIP _____

1. **OPT-OUT AUTHORIZATION**

   _____ **YES,** I want to OPT-Out. Le-Ru Telephone Co., its partners and contractors may not share information about my telecommunication services to include local service, long distance, and internet access service without permission.

2. **CUSTOMER ACCOUNT AUTHORIZATION AND PASSWORD**

   _____**YES**, I want to establish an account password

Account Password/Pin: _____ Password/pin can be any word or number or combination thereof that is familiar to you. This will need to be shared with the authorized person/persons listed on this document.

Password retrieval question: Please provide answers to the following questions in case you don't remember your password, we can still discuss your account with you or your authorized persons listed on this document.

Mother's maiden name: _____
Pet's name: _____
Where were you born? _____
What is your telephone/internet service address? _____

3. **AUTHORIZED PERSONS:** The following people are authorized for Le-Ru Telephone Co. to discuss information and/or make changes to the account.

Additional Authorized Person _____
Additional Authorized Person _____
Additional Authorized Person _____
Additional Authorized Person _____

Account Holders Signature _____ **Date:** _____

Please sign and return to our office, within 30 days:
Le-Ru Telephone Company
P.O. Box 147
Stella, MO 64867

Ways to Authentic a Customer

Customer Authentication

Pre-texting occurs when an imposter contacts Le-Ru claiming to be a customer to obtain call detail records or account information. This has become a major concern for the FCC. Therefore, the FCC now requires a customer to supply a password to receive call detail records. For access to other CPNI, such as calling feature purchases, the customer must be "authenticated" but is not required to supply a password. **Only access to call detail records requires the use of a password.**

Passwords/Pins

Passwords must be used to share call detail records. Employees are forbidden from supplying call detail records to customers without a password, even if the caller ID indicates that customer is calling from the telephone number of record. If the customer unable to supply the password or refuses to establish a password, the employee may share call details only by: calling the customer back at the phone number of record; mailing/emailing to the address of record; or confirming the identity of the person with a valid government-issued ID. Le-Ru may not supply CPNI to anyone not listed on the account unless the individual proves power-of-attorney to act on behalf of the customer. The customer must supply a password each time they call for CPNI related information.

The customer should create a password and establish back-up questions for future authentication and password prompting. This can be done in person with the proper authentication and verification or by the CSR by calling the number of record for the specific customer.

Billing Address

The customers billing address on record may be used to authenticate for CPNI that is not call detail records. This CPNI includes the quantity, technical configuration, destination, type, location, types of service purchased, and the dollar amount the customer spends on services.

Authentication Questions

The customers may also be authenticated by correctly answering one of the authentication questions they supplied. CPNI that is not call detail records can be given. This CPNI includes the quantity, technical configuration, destination, type, location, types of service purchased, and the dollar amount the customer spends on services.

Things for CSRs to Remember Regarding CPNI

1. Authenticate every customer: For example "to protect your privacy, may I confirm that I'm speaking with XXX. Could you please provide the billing address on record or can you answer an authentication question?"
2. Require a password for call detail records: For example "to protect your privacy, may I have your password in order to provide you with that information?"
3. Check Opt-Out status
4. Ask permission to discuss products and services.

If in doubt as to whether or not you will need permission, it's always better to ask for permission/passwords/authentication to look at the customer's CPNI.

In-Office Customer Visit

First, authenticate the customer with a valid government issued photo ID and confirm that the person is listed on the account or has a valid power-of-attorney form. Then check the status of the CPNI approval. Respond to the customer's request following the rules for whether or not CPNI approval is necessary. If the customer is dropping off a payment, no authentication is needed unless the customer wants to know the amount of the bill. If the person paying the bill isn't listed on the account, the amount due can not be discussed with them.

Customer-initiated Call

First, authenticate the customer with a valid password, billing address on record or authentication question and confirm that the person is listed on the account. Then check the status of the CPNI approval. Respond to the customer's request following the rules for whether or not CPNI approval is necessary.

Exceptions can not be made just because the person's name on the account is in the hospital/nursing home or even deceased. You may only discuss CPNI with authorized persons listed on the account or those with a power-of-attorney.

Account Change Notification

Le-Ru Telephone Company must notify customers immediately whenever a change is made to any of the following (not required when the customer initiates service):

- Password
- Customer response to a back-up means of authentication for password
- Online account
- Address of record

The notice can be through:

- Company originated voicemail or text message to the telephone number of record
- Sent to the postal address or email address of record

The notification must be sent in a timely manner and must not reveal the new account information or the type of information.

Sample text: "This is a notice that Le-Ru Telephone Company, as requested, has made a change to your account information. If you did not authorize this change, please contact our offices immediately at 417-628-3844."

Security

By definition, a breach means that someone, without authorization, has intentionally gained access to, used, or disclosed CPNI with the intent to do harm. If a breach happens, Le-Ru Telephone Company must:

- As soon as practicable and in no event later than 7 business days, electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through the central reporting facility. The FCC will maintain the electronic notification system at www.fcc.gov/eb/cpni.
- Notify customers and/or disclose the breach to the public but not until 7 business days have passed after notification to the USSS and FBI. These governmental bodies can request an extension of the 7 business days if it determines that customer or public notification could compromise the investigation.
- Le-Ru shall retain records of any breaches discovered, the notifications made to the USSS and FBI and customers. These records should include: dates of discovery and notification, detailed description of the CPNI that was the subject o the breach, and all circumstances surrounding the breach. These records should be maintained for 2 years.
- If the company has any breaches, these should be identified in the annual certification that is filed with the FCC.

An accidental breach would include violations like: an employee accessed CPNI and discussed services outside the customer's existing service without having received permission from the customer; employee didn't verify the customer's CPNI status; or the employee didn't properly authenticate the customer before discussing account information. These accidental violations are part of the company's disciplinary process but wouldn't be reported to the USSS or FBI. Based on the seriousness of these accidental breaches, the employee may be subject to counseling, retraining, reassignment, suspension or termination based on the severity and frequency of the breach(s).

Employee Certification
For HR File

I, the undersigned, hereby acknowledge receiving and reviewing, Le-Ru Telephone Company's CPNI Policy. I have completed the training coordinated by Le-Ru Telephone Company's CPNI Compliance Officer. I further understand my responsibilities to protect CPNI exposures and understand the disciplinary procedures in place for failing to do so.

Name:
Date policy received:
Date of training:

_____ _____

Signature Date

Witnessed by the CPNI Compliance Officer

_____

Printed Name

_____ _____

Signature Date

Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for [*Insert year*] covering the prior calendar year [*Insert year]*

1. Date filed: [*Insert date*]
2. Name of company(s) covered by this certification: [*Insert company name*]
3. Form 499 Filer ID: [*Provide relevant ID number(s)*]
4. Name of signatory: [*Insert name*]
5. Title of signatory: [*Insert title of corporate officer*]
6. Certification:

I, [*Insert name of officer signing certification*], certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company [*has/has not]* taken actions (*i.e.,* proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, provide an explanation of any actions taken against data brokers.]

The company [*has/has not*] received customer complaints in the past year concerning the unauthorized release of CPNI [NOTE: If you reply in the affirmative, provide a summary of such complaints. This summary must include the number of complaints, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____ [*Signature of an officer, as agent of the carrier*]

Attachments: Accompanying Statement explaining CPNI procedures
Explanation of actions taken against data brokers (if applicable)
Summary of customer complaints (if applicable)

CPNI Compliance Accompanying Statement

Year: *[Insert year]*

Le-Ru Telephone Company

This accompanying statement explains how Le-Ru Telephone Company's operating procedures ensure that the company is in compliance with the rules governing CPNI as found in the Subpart U – Customer Proprietary Network Information – Part 64 of Title 47 of the Code of Federal Regulations.

Le-Ru Telephone Company adheres to all CPNI rules as stated in section 64.2001 – 64.2011 concerning the proper use of our customer's CPNI. Specifically, our notice for use of CPNI approval process meets all requirements as listed in Section 64.2008. To further protect our customer's privacy, we have implemented all safeguards required in Section 64.2009. This includes:

- The implementation of a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI:
- The training of appropriate personnel as to when they are, and are not, authorized to use of CPNI and the documentation of this training;
- The implementation of an express disciplinary process for CPNI violations up to and including termination;
- The maintenance of a record, for at least one year, of our own, and our affiliates sales and marketing campaigns;
- The establishment of supervisory review process regarding carrier compliance with the federal CPNI rules for outbound marketing situations;
- The establishment of annual certification by a corporate officer with personal knowledge of Le-Ru Telephone Company's policies and procedures to ensure compliance with the federal CPNI rules;
- The establishment of procedures of notification of the Commission of any instance where mechanisms, opt-out; do not work properly, to such a degree that consumers' inability to opt-out is more than anomaly.

Le-Ru Telephone Company has attached with this document its CPNI Manual, with the sample forms, as further detailed explanation of how its procedures ensure that it is on compliance with the rules in Subpart U of Part 64, of Title 47 of the Code of Federal Regulations.

Le-Ru Telephone Company's Privacy Statement

As a current customer of Le-Ru Telephone Company, we would like to take this opportunity to both thank you for your business and to share with you the importance our company places upon protecting the privacy of information we gather from you in accordance with applicable state and federal laws. The following is Le-Ru Telephone Company's privacy policy.

Le-Ru Telephone Company collects information about our customers from the following sources:

- Information we receive from you on applications or other forms, such as your name, address, and date of birth
- Information about our customers' transactions with us, such as service requests and payment history

We do not share information about our customers or former customers with non-affiliated third parties other than as permitted or required by law.

We maintain physical, electronic, and procedural safeguards to guard your information. These safeguards include but are not limited to the following:

- We restrict access to nonpublic personal information about our customers and former customers to those employees who need to know that information in order to assist in providing services or products to the customer
- We will punish any employees who impermissibly share customer information
- We use a secure Internet and e-mail provider to protect the confidentiality of electronic communications

Le-Ru Telephone Company appreciates your business and in order to continue building upon that relationship we believe it is necessary, not only from a legal standpoint, but also as a sound business practice that our customers understand the care our company uses in handling your information. Le-Ru Telephone Company will continue to monitor the effectiveness of this privacy policy.

General Information on Red Flag Rules

Le-Ru Telephone Company recognizes that identity thieves use people's personally identifying information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. As such, Le-Ru has implemented a program to detect, prevent, and mitigate instances of identity theft for our customers.

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs provide for the identification, detection, and response to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft.

According to a report of the President's Identity Theft Task Force, identity theft (a fraud attempted or committed using identifying information of another person without authority), results in billions of dollars in losses each year to individuals and businesses.

Under the Red Flags Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs – or "red flags" – of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.

The final rules require each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor to:

1. Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks from identity theft.

Who must comply with the Red Flags Rules?

The Red Flags Rules apply to "financial institutions" and "creditors" with "covered accounts." Under the Rules, a **financial institution** is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a consumer. Most of these institutions are regulated by the Federal bank regulatory agencies and the NCUA. Financial institutions under the FTC's jurisdiction include state-chartered credit unions and certain other entities that hold consumer transaction accounts.

A **transaction account** is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

A **creditor** is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Creditors include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies (such as ABC telco). Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors. Most creditors, except for those regulated by the Federal bank regulatory agencies and the NCUA, come under the jurisdiction of the FTC.

A **covered account** is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. **Covered accounts** include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account is also an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts.

26 Red Flag Guidelines

The Guidelines identifies 26 possible red flags. These red flags are not a checklist, but rather, are examples that financial institutions and creditors may want to use as a starting point. They fall into five categories:

- alerts, notifications, or warnings from a consumer reporting agency;
- suspicious documents;
- suspicious personally identifying information, such as a suspicious address;
- unusual use of – or suspicious activity relating to – a covered account; and
- notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

26 Red Flags:

Le-Ru Telephone Company has evaluated these 26 possible red flags and identified which ones are appropriate for our operations and developed our plan to address just those realistic items. A "x" in the ☐ indicates that we potentially have this exposure.

1. ☐ A fraud alert included with a consumer report.
2. ☐ Notice of a credit freeze in response to a request for a consumer report.
3. ☒ A consumer reporting agency providing a notice of address discrepancy.
4. ☐ Unusual credit activity, such as an increased number of accounts or inquiries.
5. ☒ Documents provided for identification appearing altered or forged.
6. ☒ Photograph on ID inconsistent with appearance of customer.
7. ☒ Information on ID inconsistent with information provided by person opening account.
8. ☒ Information on ID, such as signature, inconsistent with information on file at financial institution.
9. ☒ Application appearing forged or altered or destroyed and reassembled.
10. ☐ Information on ID not matching any address in the consumer report, Social Security number has not been issued or appears on the Social Security Administration's Death Master File, a file of information associated with Social Security numbers of those who are deceased.
11. ☒ Lack of correlation between Social Security number range and date of birth.
12. ☐ Personal identifying information associated with known fraud activity.
13. ☒ Suspicious addresses supplied, such as a mail drop or prison, or phone numbers associated with pagers or answering service.
14. ☒ Social Security number provided matching that submitted by another person opening an account or other customers.
15. ☒ An address or phone number matching that supplied by a large number of applicants.
16. ☒ The person opening the account unable to supply identifying information in response to notification that the application is incomplete.
17. ☒ Personal information inconsistent with information already on file at financial institution or creditor.

18. ☒ Person opening account or customer unable to correctly answer challenge questions.
19. ☒ Shortly after change of address, creditor receiving request for additional users of account.
20. ☐ Most of available credit used for cash advances, jewelry or electronics, plus customer fails to make first payment.
21. ☒ Drastic change in payment patterns, use of available credit or spending patterns.
22. ☐ An account that has been inactive for a lengthy time suddenly exhibiting unusual activity.
23. ☒ Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account.
24. ☒ Financial institution or creditor notified that customer is not receiving paper account statements.
25. ☒ Financial institution or creditor notified of unauthorized charges or transactions on customer's account.
26. ☒ Financial institution or creditor notified that it has opened a fraudulent account for a person engaged in identity theft.

Duties of the Red Flag Compliance Officer

Le-Ru Telephone Company has assigned, Kendall Williams, as its Red Flag Compliance Officer. This person helps establish policies and procedures to detect, deter/mitigate identity theft exposures, and report them as necessary to the appropriate authorities both internally and externally.

This person is also responsible for training the other employees on ways to identify, detect, and respond to Red Flag indicators as described in this document. All employees who have identified suspicious activities as relates to these Red Flag rules should report it immediately to the compliance officer who will then take the next steps.

This person is also responsible for updating, as appropriate, the Red Flag policy of Le-Ru Telephone Company.

Certification for Red Flag Compliance Officer

I certify that I am an Officer of Le-Ru Telephone Company.

I have personal knowledge that the Company (and its affiliates) established operating procedures that are designed to ensure compliance with the Red Flag Rules of the Federal Trade Commission. I report directly to the Board of Directors in this regard as soon as possible if a noncompliance issue is red flagged.

The attached statement of Red Flag compliance explains how the Company's operating procedures ensure that it is in compliance with the foregoing FTC rules.

Printed Name: Kendall Williams
Office Held: Operations Manager

K. Williams
Signature

2-9-18
Date

Le-Ru Telephone Company's Checklist of Policies & Procedures Relating to Red Flag and CPNI Exposures

1. **MANAGEMENT OF CONTENT AND PRIVACY EXPOSURES:**
   a. Does Le-Ru collect, process, or maintain private or personal information as part of its business activities?
   ☒ Yes ☐ No

   b. Does Le-Ru have an appointed privacy officer? ☒ Yes ☐ No

   c. Does Le-Ru have a legally revised privacy policy? ☒ Yes ☐ No

   d. Does Le-Ru share private or personal information gathered from customers with third parties?
   ☐ Yes ☒ No

2. **COMPUTER SYSTEMS CONTROLS:**

   a. How many of the following comprise Le-Ru's network:
   1 Server computers
   6 Workstation computers
   6 Authorized user accounts
   1 Geographically distinct LAN sites

   b. Le-Ru has the following written information systems policies which are published and distributed to employees with a written sign-off of acknowledgement (in the policy manual/handbook):
   x "Acceptable use" Standards
   x The company's right to monitor employee computer use and activity, including reading emails and monitoring website activities
   x Acceptable email use
   x Acceptable internet use
   x Password discipline
   x Incident response, handling, and reporting
   x Standards of communication for proprietary, sensitive, and confidential materials

   c. Le-Ru conducts training for every employee user of the information systems in security issues and procedures for its Computer Systems? ☒ Yes ☐ No

d. Does Le-Ru have:
A disaster recover plan? ☒ Yes ☐ No
A business continuity plan? ☒ Yes ☐ No
An incident response plan for network intrusions and virus incidents? ☒ Yes ☐ No

e. Are Le-Ru's internal networks and/or Computer Systems subject to third party audit monitoring (including ethical hacking for security purposes)? ☒ Yes ☐ No

If Yes, a summary of the scope of such audits and monitoring is attached to the document:
See Credit Card Security Policy

3. **COMPUTER SYSTEMS ACCESS PROTECTION:**

a. Does Le-Ru provide remote access to its Computer Systems? ☒ Yes ☐ No

If Yes,
How many users have remote access? 1
Is remote access restricted to Virtual Private Networks (VPNs)? ☒ Yes ☐ No

If the answer is No, describe the extent to which other remote access is allowed such as modem dial-in accounts, Remote Access Servers (RAS), or dedicated Frame Relay (FR) communications.

_____

_____

b. Le-Ru uses the following password disciplines which are enforced via automated systems or software settings:
x Password must contain at least eight (8) characters.
x Password must contain a mix of letters and one or more numbers and/or special characters (*0&%4#S).

c. Does Le-Ru terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company? ☒ Yes ☐ No

d. Does Le-Ru use commercially available firewall protection systems to prevent unauthorized access to internal networks and computer systems? ☒ Yes ☐ No

e. Does Le-Ru use intrusion detection software to detect unauthorized access to internal networks and Computer Systems? ☒ Yes ☐ No

f. Does Le-Ru accept payment on-line for services? ☒ Yes ☐ No

If Yes,
Does Le-Ru use commercially available software to ensure that these systems are secure?
☒ Yes ☐ No

g. Does Le-Ru employ Anti-Virus software? ☒ Yes ☐ No

If Yes, is it company policy to up-grade the software as new releases/improvements become available? ☒ Yes ☐ No

4. **DATA BACKUP PROCEDURES:**
   a. Is all Valuable/sensitive data backed-up by Le-Ru every day? ☒ Yes ☐ No

   b. How long are back-up tapes stored before being overwritten? 2 Days

5. **DATA ENCRYPTION PROCEDURES:**
   Does Le-Ru have and enforce policies concerning when internal and external communications should be encrypted? ☒ Yes ☐ No

   If Yes, describe the types of 1) Internal and 2) External communications which are encrypted:

   See Credit Card Security Policy

Overview of Le-Ru Telephone Company's Plan

In response to our requirement to establish a Red Flag Policy and the specifics of the above checklist, Le-Ru Telephone Company has identified the following overview of our plan to protect personal data of employees and customers.

Principles of Data Security and Le-Ru Telephone Company's Overview of Data Security:

- Take Stock: know what personal information you have in your files (both paper and electronic) on both your employees and customers
- Scale Down: keep only what you need for your business
- Lock It: protect the information you keep—especially in high traffic areas such as CSR areas
- Pitch It: properly dispose of what you no longer need or are required to keep
- Plan Ahead: create a plan to respond to security incidents

To protect our employees, retirees, and applicants, we have established the following:

Human Resources Data Policies:

- Only authorized personnel shall have access to human resources personal information. This does not include summer interns, temps, or part-timers
- Applications (either on paper or on-line) collect just about everything an ID thief would want. So, Le-Ru Telephone Company will store all applications and human resources files in a locked "file cabinet" (including a literal file cabinet and an electronic file cabinet) which requires a key or a password to access
- The Fair Credit Reporting Act sets the standards and determines when and if reference and background checks become a consumer report and subject to Red Flag rules. Le-Ru Telephone Company follows these standards
- Le-Ru treats all communication from any consumer reporting agency as under the influence of the Red Flag rules
- Paper files are shredded on-site

As an organization, we have established the following computer network security features to mitigate and deter identity theft:

Le-Ru Telephone Company's Computer Network Security Measures:

- Firewalls and virus-protection software is installed and updates automatically
- CDs are shredded/broken to be disposed of
- Computers are set to lock (needing a password) if left unattended for 1 hour amount of time
- All smart phones and VPNs are password protected
- Passwords must contain upper and lower case letters and numbers
- No customer information will be stored on laptops or external drives
- On-line payments are encrypted
- All SSN numbers are masked on the computer screen (xxx-xx-1234) and never sent over the internet
- Investigation of "phishing" or fake emails designed to get customers to provide personal information by the IT department and/or compliance officer

Employee Responsibilities:
Le-Ru Telephone Company has adopted a clean desk rule. Employees are not allowed to leave sensitive data on their desks at the end of the day or if they are gone from their desk for a long period of time. Computer screens will not face a direction so that the customer can see the data on it. Employees will use the proper verification/authentication forms each time they touch/work-on opening, closing, adding/deleting services, or making any kind of changes to the contacts and/or the address on the primary account.

Opening and Closing and Modifying Customer Accounts:
Attached are the documents/forms that Le-Ru Telephone Company uses to open and close accounts for customers.

Le-Ru Telephone Company Information

Date: _____

No. Issued: _____

Le-Ru Telephone Company
P.O. Box 147
Stella, MO 64867

(417)-628-3844
Toll Free (866)-628-3844
Fax (417)-628-3686

Name (Listing in Directory): _____

County 911 Address (Where Phone is Located): _____

Billing Address: _____

Would you like to have Paperless Billing? Yes ☐ No ☐

How Long at this Address? _____

Previous Address: _____

Cell Number: _____ Current Email: _____

Social Security Number: _____

Spouse's Name: _____ Cell Number: _____

ployment Information

Place of Employment: _____ Work Number: _____

Spouse's Employment: _____ Work Number: _____

Other Source of Income if not Employed: _____

Location Information

Residential or Business: _____

Has there been service at this location before? Yes ☐ No ☐

Former Resident at this Address: _____

Nearest Neighbor: _____

House ☐ RV ☐

Rent ☐ Own ☐ Making Payments ☐

If Renting

operty Owners Name: _____ Telephone: _____

Telephone Bills are Due on the First Day of the Month. Past Due on the 21st.

Limitation of Liability

Company's entire liability and your exclusive remedy for damages arising out of this agreement shall not exceed the total net charges to you for service to which the ned damages relate during the period in which such claimed damages occur and continue. In no event, shall any other liability attach to Company. This limitation will not apply to bodily injury, death or damage to real or tangible property directly caused by Company's gross negligence or intentional misconduct.

Neither party will be liable to the other party under any circumstance for any indirect, incidental, consequential, punitive or special damages.

Access and Right-of-Way

The Company's obligation to furnish service is dependent upon the availability of facilities and its ability to secure and retain, without unreasonable expense, suitable facilities and rights for the construction and maintenance of the necessary equipment. The undersigned agrees to provide Company with suitable right-of-way and provide Company representatives with access to the undersigned's property at any reasonable hour for the purposes of installing, inspecting, repairing, testing, or removing any part of the Company's facilities and network.

Discontinuance of Service for Residential Customers

A. Service may be discontinued for any of the following reasons:

1. Non-payment of an undisputed delinquent charge for basic local telecommunications service.
2. Failure to post a required deposit or guarantee.
3. Unauthorized use of the Company's service in a manner which creates an unsafe condition or creates the possibility of damage or destruction to its facilities.
4. Failure to comply with the terms of a settlement agreement.
5. Refusal after reasonable notice to permit inspection, maintenance or replacement of Company's equipment.
6. Material misrepresentation of identity in obtaining Company's service.
7. As provided by state or federal law.

B. A written notice shall be sent by first class mail ten (10) days prior to the date of the proposed discontinuance of service.

C. Service may be discontinued during normal business hours on or after the date specified in the notice of discontinuance. Basic local telecommunications service will not be discontinued on a day when the offices of the Company are not open to facilitate reconnection of basic local telecommunications service or on a day immediately preceding such day.

D. Company will make reasonable efforts to contact the customer via telephone at least twenty-four (24) hours preceding a discontinuance of ic telecommunications service. The Company will advise the customer of the proposed discontinuance and what action must be taken to avoid it.

E. Discontinuance of service will be postponed for a time not in excess of twenty-one (21) days if the telephone is necessary to obtain emergency medical assistance for a person who is a member of the household where the telephone service is provided and where such person is under the care of a physician. Any person who alleges such emergency shall, if requested, provide the Company with verifiable written evidence of such necessity.

F. Basic local telecommunications service may not be discontinued for customer nonpayment of a delinquent charge for other than basic local telecommunications service. Company may place global toll blocking and eliminate any optional, non-basic calling features and functions for customer nonpayment of delinquent charges for other than basic local telecommunications service.

G. Payment by personal check may be refused if the customer, within the last twelve (12) months, has tendered pa5rment in this manner and the check has been dishonored, except when the dishonor is due to bank error.

Restoral of Service

A charge of $20.00 will be made for reconnecting services which have been discontinued for non-payment of charges due. No allowance will be made for loss of service during the period service is disconnected for non-payment if payment is made and service reconnected before completion of an order to terminate the service. Subsequent to the completion of an order to terminate the service, it may at the option of the Company be re-established only on the basis of a new application.

Late Payment Charge

The Company shall assess a late payment charge in the amount of $10.00 to cover the cost of handling such delinquent account. In the event a partial payment is made on the current bill, subsequent to the issuance of the Notice, the late payment charge will be added to the balance due.

The undersigned makes application for telephone service of the kind and class as described above, and agrees to pay the rates as established for such service, and further agrees to the rules and regulations as set forth in the exchange tariff, and to any general changes in the rules, regulations, tariffs or rates for such services. This application becomes a contract when accepted in writing by the Telephone Company.

SIGNATURE _____

DATE _____

Le-Ru Telephone Company
P.O. Box 147 | 555 Carter St.
Stella, MO 64867
Main: (417)-628-3844 | Toll Free: (866)-628-3844 | Fax: (417)-628-3686
Email: info@leru.net

Request of Service Change

I hereby request, Le-Ru Telephone Company, to make changes to my account regarding the services provided. Please change the following:

☐ Add telephone service

☐ Add Internet service

☐ Add Long Distance service

Please provide name of requested long distance service provider:

_____

☐ Disconnect all services

☐ Disconnect just Internet services

Services will be changed the day Le-Ru Telephone Company receives this document and service charges will be pro-rated from this date.

Only authorized persons who are listed on the account are capable of changing or disconnecting services. Exceptions cannot be made just because the person's name on the account is in the hospital/nursing home or even deceased. Only persons listed on the account or those with a power-of-attorney can authorize changes to the account.

Signature: _____ Date: _____

Vendors/Independent Contractors Data Security

Le-Ru Telephone Company recognizes that from time to time, we use vendors and independent contractors who may have access to data that could be used by identification thieves. As a result, we ask all of these partners to answer and return the following questionnaire. The responses to these questionnaires are kept with the Red Flag documents by the Compliance Officer.

Memorandum

To: Le-Ru Telephone Company Partners
From: Red Flag Compliance Officer
Date: _____
Re: Data Security Update

As a risk manager, we believe that understanding exposure is critical. Therefore, we are currently reviewing our data and network liability. We have analyzed our internal controls and exposures and feel comfortable with the combined protection and transfer that we are utilizing.

We also recognize that our support vendors/partners may create an exposure. So with that in mind, we are asking you to respond to the questions on the attached page, so we can determine how to best manage the risk of the data that is in your control. Please fax back the questionnaire by xxx to xxx.

Our company name, for your records, is _____.

We value our relationship with you and are seeking to make sure that we are both protected from this emerging concern.

Please let me know if you have questions. My contact information is:

_____

Company Name: _____

Contact Name: _____

1. Do you assume responsibility for a breach of any or all of Le-Ru Telephone Company's data that your company handles as part of our relationship? Please explain.
   □ Yes □ No

2. If you are using subcontractors have your determined if they are assuming liability for network security and data breaches? Please explain.
   □ Yes □ No

3. When was your company last audited with regard to network security and data liability?

4. If you have not had an audit is one planned and if so when?
   □ Yes □ No

5. Do you have a written policy on network and data security?
   □ Yes □ No

   If yes please supply a copy of the document.

6. Do you purchase insurance for this risk?
   □ Yes □ No

   If yes, please provide the name of the insurer, effective date of coverage and limit of protection. Please also confirm that your policy provides coverage for data that is in your care, custody and control.
   Insurer:_____

   Effective Date: _____

   Limits: _____

7. Please identify your security compliance officer and their contact information:

Thank you for completing this form.
Please return via fax to our offices at 417-628-3686.

Red Flag Training Topics
Suspicious Items that Warrant Additional Screening

Le-Ru Telephone Company has provided training to our employees to help identify potential Red Flags and to protect our customers, employees-past and present, and our vendor relations. The following are some of the topics that received training. If a CSR or person opening/closing/modifying an account encounters any of these items that gives them reason to be suspicious, they are to immediately notify the Red Flag Compliance Officer.

1. Alerts, notifications, or other warnings from consumer reporting agencies:
    a. a fraud or active duty alert is included in a consumer report
    b. a consumer reporting agency provides a notice of a credit freeze
    c. a consumer reporting agency provides notice of address discrepancy
    d. a consumer reporting agency indicates a pattern of activity that is inconsistent with the history or usual pattern of activity for the applicant or customer such as:
        i. recent/significant increase in the volume of inquiries
        ii. unusual number of recently established uses of credit
        iii. material change in the use of credit
        iv. account was closed for cause or identified for abuse by a financial institution/creditor
2. Presentation of suspicious documents:
    a. documents presented for identification appear to be altered or forged
    b. photograph or physical description is not consistent with the actual appearance
    c. other information on the identification is not consistent
    d. Information is not consistent with information already on file
    e. application appears to have been altered or destroyed
3. Suspicious Personal Identifying Information:
    a. Personal identifying information is inconsistent when compared to external sources (Ex: address does not match the address on the consumer's report; SSN has not been issued or is listed on the SSA's death master file)
    b. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or 3rd party sources (Ex: address is fictitious; phone number invalid)
    c. SSN is the same as that submitted by another
    d. Address or phone number provided is the same as or similar to an account submitted by an unusually large number of persons
    e. The person opening/closing/modifying the account fails to provide all of the personal identification/authentication information
4. Unusual Use of or Suspicious Activity Related to the Covered Account:
    a. Shortly after a change of address request, the telco receives a request for new/additional/replacement goods and/or services
    b. Shortly after a change of address request, there is a request for additional authorized users
5. A covered account that has been inactive for a lengthy period of time is used
6. Mail sent to the address of record repeatedly is undeliverable although transactions continue to be conducted

7. Le-Ru is notified of unauthorized charges/transactions on a covered account
8. Le-Ru is notified by the customer or the law enforcement or the victims of ID Theft regarding a covered account
9. Monitoring multiple authentication requests from the same IP address is important

Company Communication Policy

Corporate communication may take various formats including but not limited to the following: written, verbal, phone, fax, electronic mail (defined as any non-paper mail that is transmitted to or from the Company or its employees), and the Internet. As the corporate image is displayed in all of these formats, Le-Ru Telephone Company expects high standards of professionalism in all of its communications. All forms of communication to and from the employees of the organization, whether written, oral, or electronic, are therefore considered property of Le-Ru Telephone Company and may be retrieved, monitored and read at any time. Employees should not use a password, access a file or retrieve any stored communication without authorization.

Computers, computer files, the email system and software are Company property intended for business use.

Much of the information accessed over the internet is protected by copyright and copying could violate federal law and therefore is not acceptable from company computers without permission of the owner. Respect copyright, fair use, privacy, and financial disclosure laws.

Internet users may not send or receive any form of derogatory or harassing remarks, including comments on age, disability, national origin, political affiliation, race, religion, gender, sexual orientation or some similar distinction. No sexually oriented or pornographic or obscene material may be transmitted to or from your company owned computer.

Employees are required to follow Company guidelines with regard to computer maintenance, anti-virus updates, and internet security and passwords.

Blogging, wikis, and other forms of online discourse are individual interactions and not intended to be corporate communications and should not be done on company computers. If you blog on your personal computer and mention Le-Ru Telephone Company, you must make it clear that you are speaking for yourself and not representing the Company. Do not provide customer, partner, Shareholder, Board, or Association proprietary information without their express written permission.

Abuse of Internet access provided by the Company in violation of law or Company policies will result in disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violation of this policy. The following are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action: sending or posting discriminatory, harassing, or threatening messages or images; using the organization's time and resources for personal gain; stealing, using, or disclosing someone else's code or password without authorization; copying, pirating, or downloading software and electronic files without permission; sending or posting confidential material, trade secrets, or proprietary information outside of the organization; violating copyright law; failing to observe licensing agreements; engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions; sending or posting messages or material that could damage the organization's image or reputation; participating in the viewing or exchange of pornography or obscene materials; sending or posting messages that defame or slander other individuals; attempting to break into the

computer system of another organization or person; refusing to cooperate with a security investigation; sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities; using the Internet for political causes or activities, religious activities, or any sort of gambling; jeopardizing the security of the Company's electronic communications systems; sending or posting messages that disparage another organization's products or services; engaging in any other illegal activities.

Le-Ru Telephone Company's Employee Certification
For HR File

I, the undersigned, hereby acknowledge receiving and reviewing, Le-Ru Telephone Company's Red Flag Policy. I have completed the training coordinated by Le-Ru Telephone Company's Red Flag Compliance Officer. I further understand my responsibilities to protect Red Flag exposures and understand the disciplinary procedures in place for failing to do so.

Name:
Date policy received:
Date of training:

_____ _____

Signature of Employee Date

Witnessed by the Red Flag Compliance Officer

_____

Printed Name

_____ _____

Signature Date