

Rail Employer Reporting Instructions
Part VIII - Employer Reporting System (ERS) Internet User Instructions
Chapter 9: Security Guidelines

Introduction

The site, <https://secure.rrb.gov/ERSNet/login.aspx>, is an official United States Government site intended for use by employers covered under the Railroad Retirement and Railroad Unemployment Insurance Acts in filing service and compensation reports with the Railroad Retirement Board and related activities. The site is referred to as the Employer Reporting System (ERSNet). The Railroad Retirement Board (RRB) is taking all reasonable measures to ensure the security of the information sent and received via the ERSNet site.

Transmission Security

RRB.gov/ERSNet utilizes a secure transmission protocol (Secure Sockets Layer – SSL) to provide encryption protection for the communication between your computer and the server that RRB uses for the Employer Reporting Internet site. You will note that the address to the site begins “https” rather than “http”. This indicates you are connecting to a secure site using Secure Sockets Layer.

Authentication of User

The RRB uses a written application form to ensure that only authorized users have access to the system. The application is signed by an authorized representative of the employer and reviewed by the RRB. Once authorized, future authentication is controlled by a logon and password. A logon, if used to file forms, has the same status as a signature on a paper document.

Password Security

It is the responsibility of each individual to keep secure the password supplied for the purpose of accessing the RRB employer site. In applying for access, you agree not to share your password and to log onto the system only as yourself. All individuals requiring access to the system should apply for their own access. Users are responsible for all use of their password accounts. The system will prompt you to change your password every 60 days. If you do not access the system that often, you will be prompted to change your password upon accessing the system but in no case will passwords remain active longer than 200 days.

Secure Your PC

It is the responsibility of each individual to secure their personal computers. When you step away from your computer, it is important to lock or turn it off so that unauthorized persons cannot use your computer to masquerade as you and gain illegal access.

Password Lockout

If you type your password incorrectly more than three times, you will be temporarily locked out of the ERSNet system. If you are locked out or suspect that your password may have been compromised, contact the password administrator (312) 751-4992.

Rail Employer Reporting Instructions
Part VIII - Employer Reporting System (ERS) Internet User Instructions
Chapter 9: Security Guidelines

Password Termination

When an employee who has access to this system, leaves your company, notify the RRB to terminate their access by completing Form BA-12, Application for Employer Reporting Internet Access. Forms should either be mailed to the address listed under Section E or faxed to (312) 751-7123. If you suspect an employee is, or may become, a security problem, immediately call the password administrator at (312) 751-4992. The RRB has the capability to lock out users on a temporary or permanent basis.

Session Timeout

For security reasons, a session will not remain open indefinitely. Twenty minutes of inactivity will result in an open session being deleted. Any data entered to a screen but not “updated” or “approved” depending on the options for that screen, will be lost when a session is deleted.

Privacy and Law Enforcement Investigations

The RRB is committed to protecting privacy. Any personal information you provide as part of the application process will be used only for the purposes described. Your logon and password control confidentiality of employer data by making available only information you are authorized to receive. System administrators will not read files unless absolutely necessary in the course of their duties and will treat the contents of those files as private information at all times.

The ERSNet system maintains statistical information concerning network traffic flow and volume including date, time, Internet protocol, type of browser and operating system. We do not collect personal information about you just because you visit the site. An attempt to identify individual users will be made if, and only if, illegal behavior is suspected.

For site security purposes, we have software that can identify users. If illegal behavior is suspected, this software could be used to:

1. trace the source of an attack designed to disrupt the site,
2. trace the source of an unauthorized attempt to modify information stored on this system,
or
3. prove whether fraud has occurred in connection with a law enforcement investigation.

Use of this system constitutes consent to such tracing and auditing.

Unauthorized or Fraudulent Use

Any person who knowingly and willingly:

1. makes any representation that is false
 - a. to obtain information from RRB records and/or,
 - b. intended to deceive the RRB as to the true identity of an individual; or

Rail Employer Reporting Instructions
Part VIII - Employer Reporting System (ERS) Internet User Instructions
Chapter 9: Security Guidelines

2. obtaining unauthorized access and/or modifies information on this site, could be punished by a fine or imprisonment, or both.

Cookies

This site uses temporary session “cookies” to give you a single, uninterrupted session when you are online. This allows you to move from one secure section to another without having to re-enter your logon and password. We do not use persistent “cookies” which are permanent files placed on a visitor’s site to allow a website to monitor a visitor’s use of the site. To the extent we use any cookies; they expire and are immediately deleted no later than the closing of the Web browser.