ESS Security Statement

Once you begin the login process to our online Employee Self Service system (ESS), the exchange of information over the Internet is encrypted. Encryption scrambles the information exchanged between your browser and ESS. Your internet browser establishes a secure session with our servers.

How Encryption Works

The **secure session** is established using a protocol called **Secure Sockets Layer (SSL)** Encryption. This protocol requires the exchange of what are called public and private **keys**.

Keys are random numbers chosen for that session and are only known between your browser and our server. Once keys are exchanged, your browser will use the numbers to scramble (**encrypt**) the messages sent between your browser and our server.

Both sides require the keys because they need to descramble (**decrypt**) messages received. The SSL protocol assures privacy, but also ensures no other website can "impersonate" your financial institution's website, nor alter information sent.

To learn whether your browser is in **secure mode**, look for the secured lock symbol at the bottom right of your browser window or next to the address bar for Internet Explorer releases 7 & 8.

Encryption Level

The numbers used as encryption keys are similar to combination locks. The strength of encryption is based on the number of possible combinations a lock can have. The more possible combinations, the less likely someone could guess the combination to decrypt the message. For your protection, our servers require the browser to connect at 128-bit encryption (versus the less-secure 40-bit encryption).

Time Out Features

For additional security features, your ESS system will "timeout" after a specified period of inactivity. This prevents a curious person from continuing your ESS session if you left your PC unattended without logging out. We recommend that you always sign off (log out) when done with you ESS session.

Authorization Features

It is important to verify that only authorized persons log into ESS. This is achieved by verifying your user id and password. We allow you to enter your password incorrectly three times; too many incorrect passwords will result in the locking of your ESS user id until you call the Oakland School Help Desk (2060) or submit a Help Desk Ticket to reinitialize your user id and password. Keep your password confidential. No one should ever ask you for your password. Your password is stored encrypted in the ESS system and cannot be viewed by anyone.

You play a crucial role in preventing others from logging on to your account. Never use easy-to-guess passwords. Never reveal your password to another person. You will be required to change your password every 30 days. Your password must be at least 6 characters long with a special character (@, $, #, % or -) and a number.

Network Security Features

Various access control mechanisms, including firewalls, intrusion detection and anti-virus, monitor for and protect our systems from potential malicious activity. Additionally, our ESS servers are fault-tolerant, and provide for uninterruptible access, even in the event of various types of failures.

Security Steps You Can Take

Basic Security

Keep your password confidential. Change your password regularly and avoid using obvious personal information. Make it a regular habit to log out of your online ESS system.

Virus Management

Your Oakland Schools issued computer is updated on a regular basis with the latest virus protection software. Keep your home computer updated on a regular basis with the latest virus protection software.

PC Software

Ensure your browser is using the highest encryption available (currently 128-bit).

Communicating with Others

Regular non-encrypted Internet e-mail is not secure. Provide only non-sensitive and non-confidential information in an e-mail request or response. The Help Desk will never ask you for sensitive or confidential information via e-mail. ESS allows you to download information. Use caution in sending any sensitive information through e-mail.

Laptop Management

As a computer user, you are responsible for protecting your computer and the information you store on it. Use caution in saving downloaded ESS information on your computer. Before traveling offsite with a laptop, recognize the risks of storing information on the C Drive that is classified as “restricted” or “confidential”. During non-business hours, log off and power down your computer. During business hours, lock your computer when you are away from it.