Your Eagle System stores and collects data that is vital to your business.

Protecting that data and making sure that only authorized personnel can access it, should be a top priority.

Before ironing out the details of security implementation, it is important that you understand the basic security concepts in Eagle.

These include requiring a System sign on, tracking clerk activity in Point of Sale, utilizing role-based security and manager overrides.

Let's start with signing on to use the Eagle.

Since applications are launched through the Eagle Browser, requiring sign-on into the Browser is the first step in controlling access. This is done through setting up special security in Options Configuration.

Notice that when I open Eagle Browser to start the process, I'm asked to sign on.

To require this sign on in your Eagle Browser, open the 'System Management' Menu and then the 'Options Configuration' Menu to launch 'Options Configuration'.

You can also type 'OPT' in the Launch bar and press Enter.

Option 520 sets the 'special security' for terminals. To locate this option, press ID.

Then type '520' in the box, and press enter.

As you can see, searching by ID may bring up more than one option with the same number. Locate the option for Terminal's special security, and click in the Current Value field.

Now click the drop-down arrow. A window opens describing each selection.

We strongly recommend requiring a user to sign on every time Eagle Browser is launched. This is option 'S'.

Select ‘S’ from the drop down list and click ‘Change’.

Notice that this option is terminal specific. This means that you must set it for each terminal in your business.

Each time Eagle is opened, everyone will now be required to enter their user name and password. Only access to those functions outlined in their role, which we will discuss later, will be permitted.

When the Eagle Browser is closed, the user is automatically signed off.

Another decision that will have to be made is how your clerks will sign in to point of sale.

Best Practice requires that each clerk or anyone using point of sale sign in to each transaction.

When Point of Sale launches, the employee signs in with their user name and password.

After completing a sale, the username remains but the employee has to re-enter the password.

If a different clerk needs to sign on, he or she would simply press clear and sign on with their user name and password.

There are several ways to configure these settings so be sure to review the attached document called ‘Security Concepts Options’ located in the course materials section for this Training on Demand class.

Now that you’ve seen how you can control access to Eagle and Point of Sale, let’s see how Role-Based Security offers you more control within individual modules and functions.

A role is simply a set of permissions—also known as security bits—that give access to applications needed for a particular job.

Roles can also limit access, preventing users from viewing certain parts of the system or taking actions they are not authorized to complete.

Once signed on to Eagle, access is limited by the permissions associated with each specific role.

To maintain these roles, Open ‘Security Maintenance’, and then ‘Role-Based Security Maintenance’ to launch the Assignment Viewer.

Click the ‘Misc’ button in the ribbon menu and choose ‘Maintain Roles’.

You’ll use this viewer to add, delete or change roles for your business.

We have made setting up Role-Based Security much easier by providing several pre-built roles.

Scrolling through this list, you see a variety of roles for both clerks and managers in accounts payable, inventory, and point of sale.

These can be used as is, or you can modify them to meet your needs by adding or deleting security bits. Of course, you can also create unique roles from scratch.

An important benefit of role-based security is flexibility. As your employees develop their skills and grow into new jobs, you can easily assign a new role. For instance, an employee might move from ‘Point of Sale Clerk’ to ‘Point of Sale Lead’. All you have to do is assign the new role to them.

You can even add multiple roles from the Assignments Viewer.

Let’s say that one of your employees needs access to many different parts of the Eagle, including point of sale, inventory, and purchasing and receiving.

You can easily assign that person more than one role.

For those of you with multiple stores, you can activate the roles in one or more stores.

Special security bits known as ‘Manager Override Bits’ can help you monitor activity at point of sale.

When an override bit for a particular situation is added to a clerk role, it triggers a requirement for a manager's authorization before the transaction can continue.

For example, if a customer who has exceeded his credit limit tries to charge something, the system checks for the override bit and then prompts the clerk for a manager's Username and Password.

The manager can then review the customer's status and make an informed decision about whether to allow the transaction to continue.

Overrides such as these can be performed at the Point of Sale terminal or from a remote location.

As you can see, the security provisions in your Eagle provide some easy to use tools to protect your data.

By introducing the requirement of passwords, creating user Roles and alerting management to potential point of sale issues, you can stay in sync with security best practices.