

**SecureAware®**

# SecureAware Policy Manual

Applies to SecureAware version 3

Document date: November 2009

## **About this document**

This manual is your guide to using the SecureAware Policy module. As well as a detailed description of the module and its functions, the manual offers you guidance and provides tools to help you construct your own comprehensive security policy from the ground up.

# Table of contents

SecureAware Policy Module .....	3
Policy .....	4
Quick Start Guide .....	4
Managing the policy set.....	5
The general policy outline .....	9
Rules .....	11
Organizing your rules .....	11
Editing the contents.....	12
Standard Mapping .....	15
Find and Replace.....	16
Procedures .....	18
Creating your procedures .....	18
Linking procedures to rules.....	20
External Links .....	21
Strategy .....	22
How do the end users see the policy?.....	23
Policy Management.....	25
The Rule Library.....	26
Policy Structures.....	30
Policy Templates.....	32
Managing the company’s policy .....	34
Copying a policy (import and export).....	36
SecureAware’s logging facilities.....	37
Contact Information .....	38

# SecureAware Policy Module

A SecureAware Policy set consists of three or four levels.

Shown as the top level of the policy pyramid, the first level – **Policy** – is a comprehensive general policy and strategy document that outlines your company’s overall security policy. This top module also allows you to create an Information security handbook.



The middle level – **Rules** – contains functions which allow you to describe the rules and regulations contained in your organization’s general policy (or policies). For example; ‘Our company backs up data daily onto the server’.

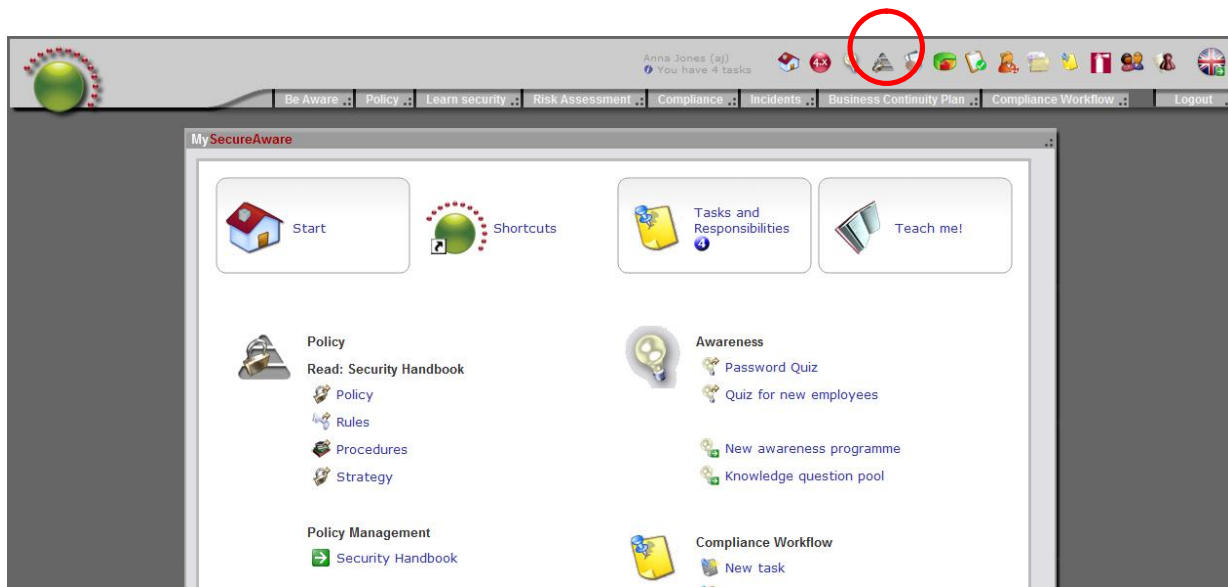
The bottom level – **Procedures** – covers actual step-by-step procedures. These procedures facilitate policy implementation and ensure that rules are complied with. For example; ‘Here is how we back up our information onto our server’.

If you have an extended SecureAware licence, your policy offers a fourth level - **Strategy**. This can be given a name of your choice and may be used for describing areas of responsibility, principles or other content which is not logical to list in other areas.

SecureAware Policy contains a range of standard templates which you can use as a basis for your own organization’s tailor-made security policy. In addition, the program allows you to define your own layouts and templates.

# Policy

The policy pyramid is shown as the second icon from the right at the top of your screen. There is also a shortcut to the module located on the opening page My SecureAware under the tab **Shortcuts**.



When you click on the icon, the following Policy Management main menu will appear. This menu is the key to creating and editing all policies, rules and procedures in SecureAware.

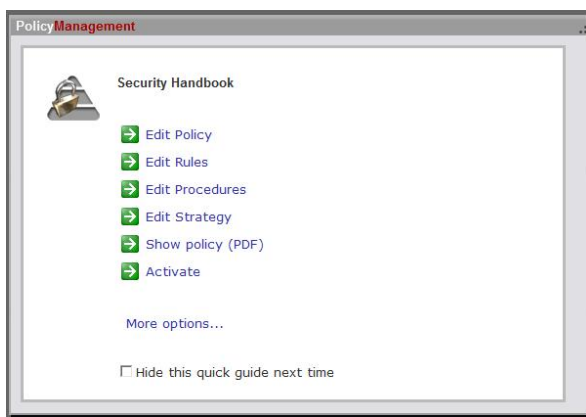
## Quick Start Guide

This step-by-step quick start guide lets you quickly and easily set up the basic framework of all your security policies. If, however, you prefer to go directly to the full Policy Management menu click on [More options...](#) A description of the full



Policy Manager is provided in the following chapter of this manual. If you choose to disable the Quick Start Guide completely, tick the **Hide this Policy Quick Guide Next Time** box (you can reactivate it at any time in the policy Manager main menu).

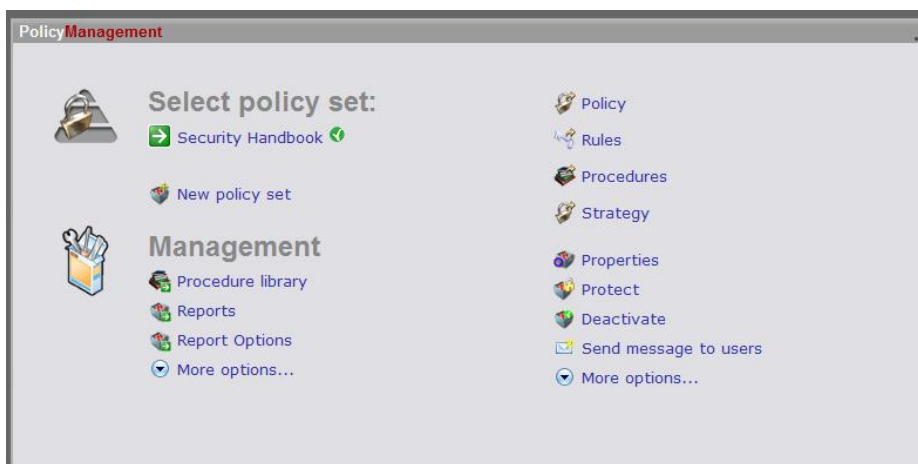
Click on **New policy set** and enter the name you wish to call your policy set and a brief description, if desired. Now click on **Next** and select the template upon which you wish your new policy set to be based. Once you have made your choice, click **Create**. Now you have a standard policy set which you can begin to customize. In SecureAware all policies consist of main policy sections, an associated list of rules a number of set procedures, and, if applicable, a fourth level – Strategy. All of these elements can be edited and tailored directly using the Policy Quick Guide. How to do this is described below.




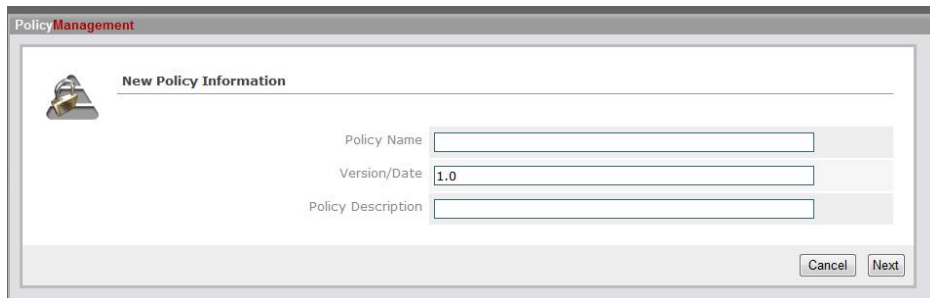
You can view all these policy elements at any time by clicking on **Show policy**. The desired policy will now be shown in PDF format in its current form. By clicking on **Activate** the policy set will be accessible to users.

## Managing the policy set

If you choose to deactivate the Policy Quick Guide you will be taken directly to the main Policy Management menu each time you open the Policy module (shown below). This menu gives you the full range of policy editing and managing options for all your policies, rules and procedures in SecureAware.

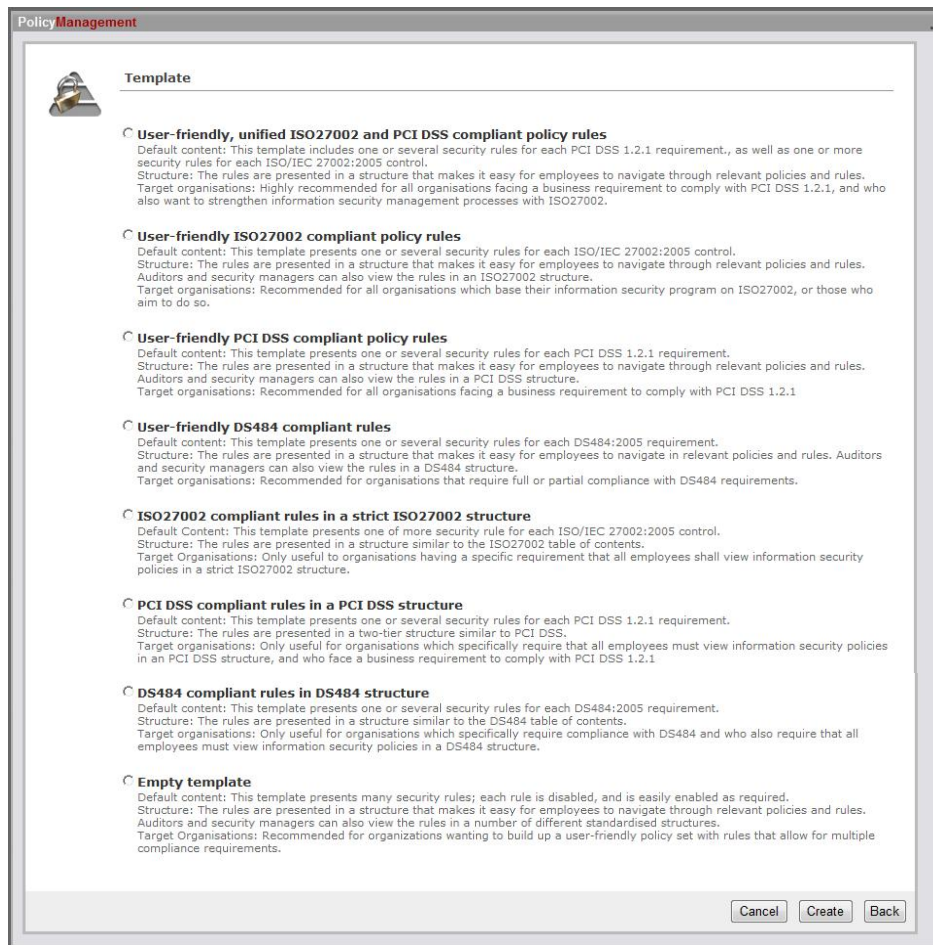


To create a new policy set from here, click on  **New policy set**. You will now see the screen shown below. In this screen, you can enter a name and give it a brief description.





Click on **Next** to go on.

Now you can set up your policy set using one of the incorporated standards as a template. You can also use a blank template if you want to define the layout of the policy set yourself. If your company is required to meet a certain standard (or even parts of an established standard) such as ISO27002:2005 or PCI, we recommend that you use one of the standard templates. The other templates do not necessarily follow these set standards' structures but contain the same rules in a more user friendly structure.




Once you have selected which policy template you wish to use, click on **Create**.

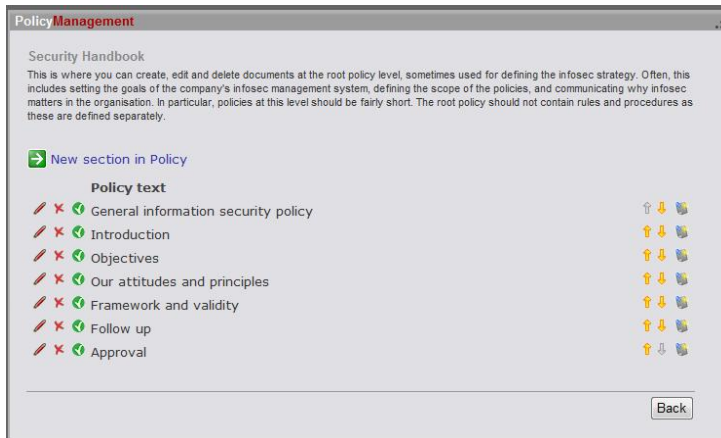
The policy set that you have created will now be listed under **Policy Sets** heading in the Policy module main menu. The green arrow  to the left of the policy set name indicates which policy set is currently subject to editing. If there is more than one name, the others will be shown with a grey arrow. Any changes you make will only affect the policy set with the green arrow. To choose a different policy set, click on the grey arrow (which now will change to green).

The green tick to the right of a name  indicates that a policy set is 'active'. It is this policy set that end users will see when they log on to SecureAware and select the Policy tab in their menu.



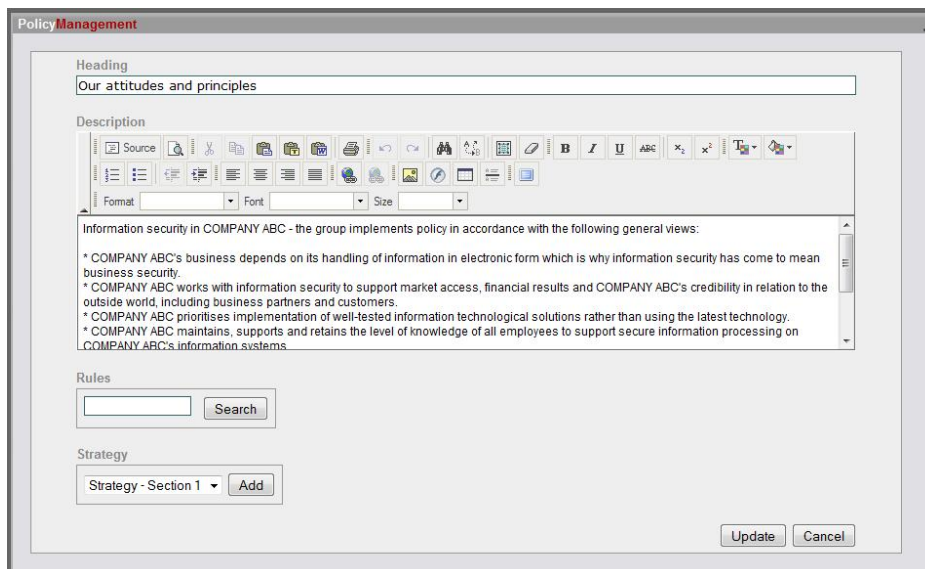
As a standard setting, the first policy set you create will become active. To change this, click on the name of the policy set you want (it gets a green arrow). Now click on  **Activate** on the list on the right-hand side of the main menu. The selected policy set will now become active.

# The general policy outline



Clicking on **Policy** lets you see general policy and strategy outline (the one currently active at that point in time). You can choose to delete aspects of this policy by clicking on ✖, or merely deactivate one or more aspects by clicking on the tick ✔. You can also alter the order of information using the yellow arrows ⬆️⬆️⬆️⬆️⬆️⬆️⬆️⬆️⬆️⬆️. To add a new

section, click on ➡️ **New section in Policy**.



To edit a particular policy aspect, click on the pencil ✎. The screen will now show a text that relates to that particular aspect of the policy. The standard default company name used throughout this module is 'COMPANY ABC'. As a minimum, you will be required to change this to your own company name.

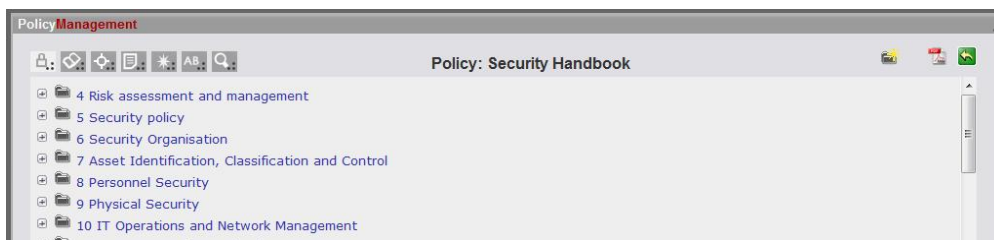
You can also alter the title or format the text. Use the editing tools at the bottom of the screen to do this. Once you have completed editing the text, click on **Update**. If you regret your changes, click on **Cancel**.

At the bottom of the screen, you can search for and create links to rules which may be relevant to this specific aspect of the main policy. Links to Strategy can also be inserted into this level.













# Rules

The different rules that together constitute your rule set can be managed by clicking on [Rules](#). Unlike the general policy outline, these rules explain in detail what a person may or may not do in respect to a company's information security policy.




As shown below, these rules are divided into security categories (shown as folders). An ISO 17799:2005 template has been used in the example below. As a result, the security categories are set out and numbered in the same order as this international standard. You can alter, delete or add to the different categories here.




## Organizing your rules

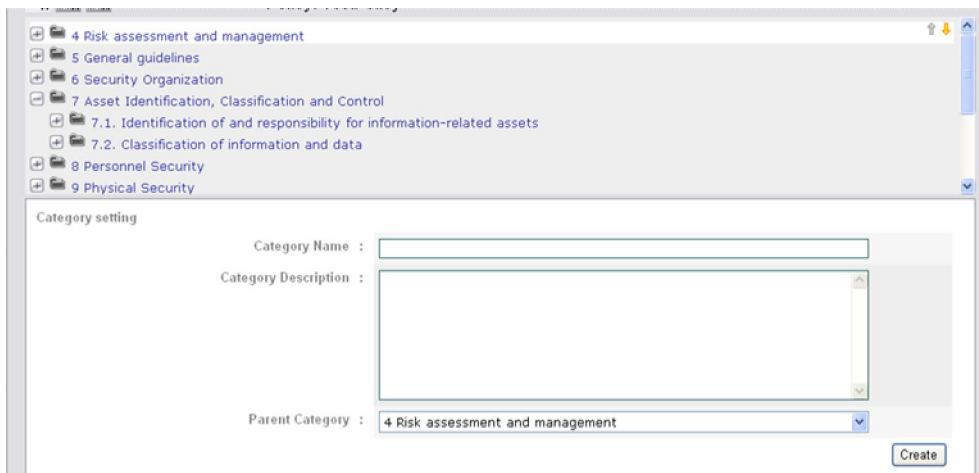
At the top left of the Policy Management screen you will see a menu which allows you to sort and organize your rules      . In the standards setting, the rules are listed according to their security category , but you can also choose to list them according to their content by clicking on . If you want your rules to be listed according to which target group they are aimed at (End user/IT administrator/management) click on . By clicking on  you can view the rules listed according to the standards to which they relate. The  icon lets you sort the list alphabetically and the  allows you to search within the rules (the search is carried out according to the name of the rule).

## Editing the contents



In the top right corner you will see four editing icons. You can return to the main menu using . The right PDF icon is used for standard mapping (described in a later section). To create a new category, click on  (see below). Click on  to add a target group to all your rules. Adding the target group to rules may have an effect on other Policy sets if they use the same rules.

### Creating new categories

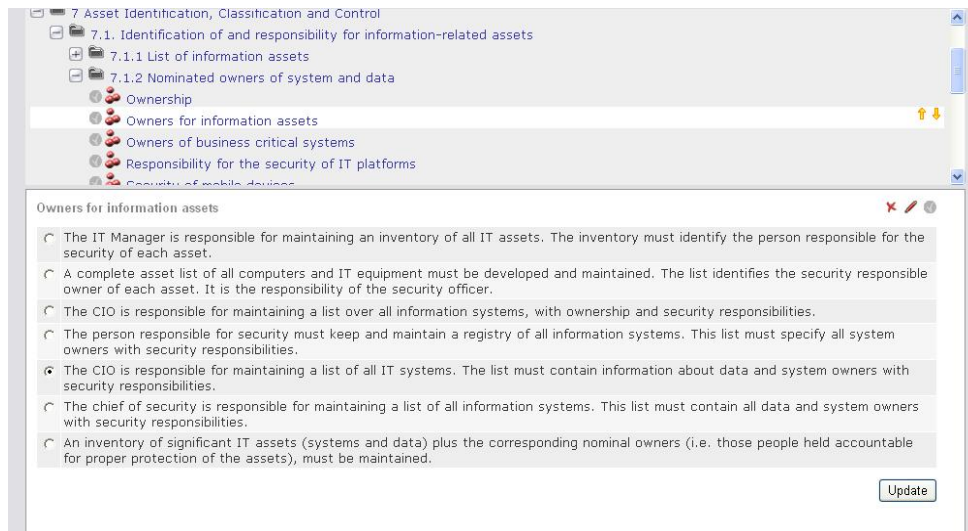
The categories shown in the policy template can be deleted or altered to meet your specific requirements. You can also create and add new categories and subcategories to your layout. If you want to create a new category, click on . Enter a new category name and any description you require. If you want your new category to be a subcategory of an existing rule use the **Parent Category** drop-down menu. End by clicking on **Create**. Once your new category has been created, you can change its position. (Note that you can only move the new category within a policy of the same level.)







### Creating new rules

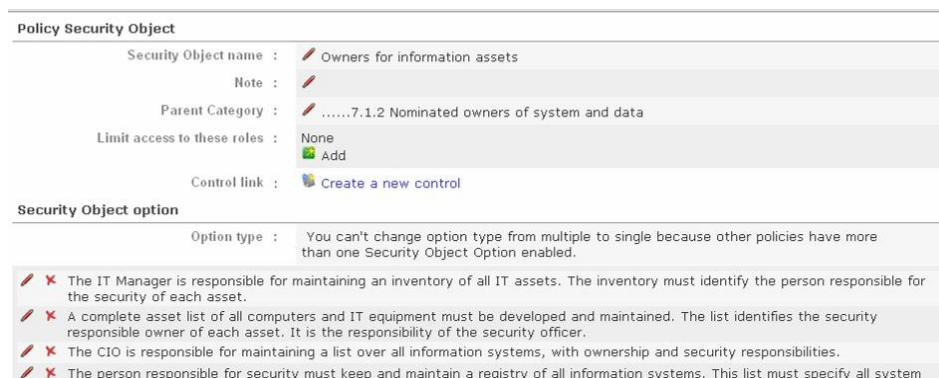
Clicking on  expands a category allowing you to view its subcategories and associated rules. By further clicking on , you will be presented with a selection of rules (and options). Below you can see the options that are listed under the **Risk assessment and management** rule. Some of these

options are marked with a tick whereas others aren't. Only the ticked options will be included in your policy. Click in the box to the left of a rule to include or remove an option.



If you want to create your own option or alter the wording of an existing option, click on  to edit. (In the example here, we are editing the General risk assessment subcategory). By clicking on  to the left of each option, you can change the wording and by clicking on , you can delete it completely. Note that you don't need to delete an option or rule to prevent it from being listed in your policy rules – deactivating it is sufficient.


To create a new option, click on  **Add** at the bottom left of the screen and then enter your text in the box. When done, click on **OK**. In the same way, you can alter a rule name, add a comment, or change the category under which it is listed.





### Links to other sections of the policy

In order to link to procedures or other sections of the policy (or, if applicable, to the fourth layer) click on Add, select to what you wish to link and click OK, Now, when end users are shown this rule they will also be given a link to the related procedure or main policy section.

### Target groups and topics


Similarly, you can allocate a rule to a topic or target group. By doing so, it becomes easier for the end user to find rules specifically relevant to them (target group) and to search for that topic under which the rule belongs. Click on  in the top right corner of the screen to add a target group to all your rules. Adding the targetgroup to rules may have an effect on other Policy sets if they use the same rules.


### Adding a rule to a category

If you want to list particular rules under a specific category begin by marking the category desired. As mentioned, the rules are listed as options so you must now locate the option you wish to incorporate. Click on  in the top right corner. You will now be presented with a searchable list of existing options (it isn't necessary for you to write the entire name when you are searching). If your search results in multiple matches, select the one you require by clicking on . If you aren't sure which match contains the precise rule you want to use, add all of them and then subsequently delete the ones you don't need.




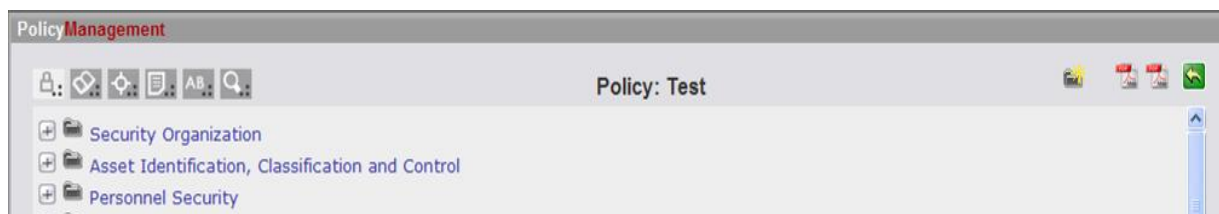
Once you have done this, click on the rule to display its options and tick the ones you wish to include. Click **Update** to save your changes.

If you want to create an entirely new rule, mark the category you want it to be listed under and click on . Now you will be able to give your new rule a name and description. Click on **Create** when

done. Now you can edit the rule in the same way as the existing rules by clicking on . (See the ‘Creating new rules’ section).

## Standard Mapping

You can use SecureAware’s standard mapping function to get an overview of how well your rules conform to a given standard. Open the Policy Management module using the  icon at the top right of the screen and click **Rules** section. Open the Standard mapping using the right PDF icon in the top right corner.



Now select the standard with which you wish to compare your rules. You can choose between DS484:2005, ISO17799 or PCI DSS (Payment Card Industry Data Security Standard). Now, select either Full Report or Gap Report (a description of these report types is given below) and click on **OK**.



You will now be shown the report’s properties. Click **Back** to change this, **Return** to cancel or **Show report** to generate and view the report.

### Full Report

#### 7.1 Responsibility for assets

##### 7.1.1 Inventory of assets

###### Registration of IT equipment

- All IT equipment is to be registered with owner, serial number and current location.

###### Identifying business critical functions

- All business critical functions, related processes, systems and owners must be identified and documented.

###### Administration of domain names

- The responsibility for registration of domain names lies with the IT Manager.

##### 7.1.2 Ownership of assets

###### Owners of business critical systems

- All critical functions requiring special knowledge, skills or experience must be identified, and have to be assigned a responsible owner.

###### Responsibility for classification

###### Responsibility for access rights

- The system data owner is responsible for establishing access rights and reassessing access rights on an ongoing basis in accordance with the company’s general access policy.

If you choose Full Report, you will be shown all sections within the selected standard followed by a list of the associated rules in your active policy.

## Gap-report

### 7 Asset management

#### 7.1 Responsibility for assets

##### 7.1.2 Ownership of assets Ownership

##### 7.1.3 Acceptable use of assets Configuration of web browsers Senders and receivers Exchanging information with third parties

If you choose Gap Report, you will be shown a list of the sections within the selected standard that DO NOT relate to your policy. You will also be offered a list of suggested rules that you could consider including in your policy.

## Find and Replace

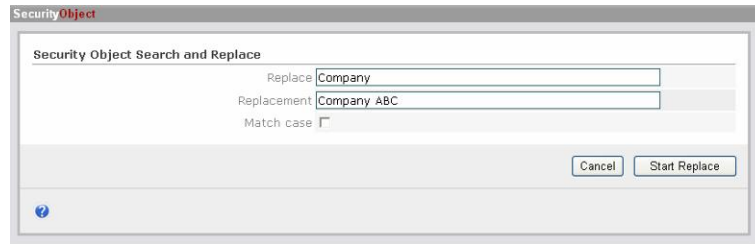
As mentioned earlier, you can edit the text of any rule by locating the required text and carrying out a manual edit using the edit function. In many cases, you may find it to be simpler to use the module's Find and Replace function. An example where this could be beneficial could be if you wish your rules text to include your specific company name (as opposed to merely being referred to as 'the company' as the first example below shows).

The company has the means and right to filter and limit access to Internet.

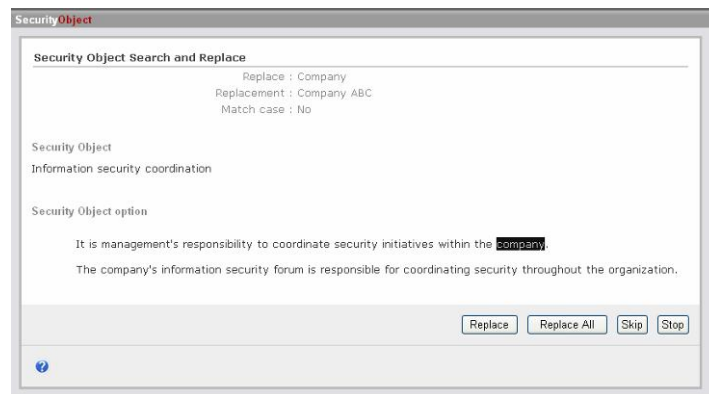
Can be changed to:

ABC company has the means and right to filter and limit access to Internet.

In the left-hand Management menu, start by selecting [Rule library](#). Now select the **Search and Replace** icon in the top right-hand corner. Now enter the word which you wish to change and the word or words you wish to set in its place. This function also allows you to refine your search according to upper or lower case text. When ready, click **Start replace** to begin.



You can now decide whether you want to automatically replace all matches or be shown each match one by one for you to approve on an individual basis. This second option is usually most advisable as an automatic **Replace all** will not take into account grammatical aspects such as plurals or tense.



# Procedures

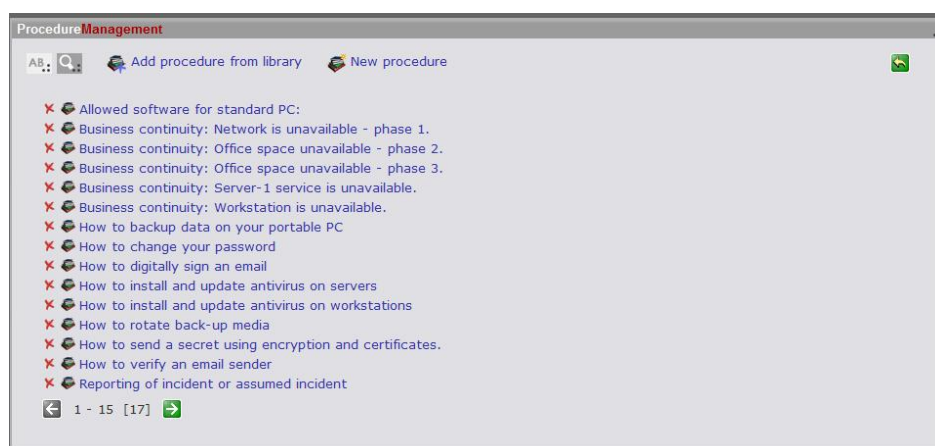
You have now put together and edited the set of rules you want your policy set to include. Now you can begin to set out the set procedures that need to be followed in order to ensure that these rules are adhered to correctly. In the standard setup, there are no procedures listed under the rules. Instead, there is a wide selection of working-practice examples for you to choose from. All of these can be edited and tailored to meet your individual needs.

Procedures give practical guidance and tell an end user how to comply with a specific policy rule. For example, for the rule “Your password must be changed every 90 days” you could incorporate a procedure which is called “How to change your password”.

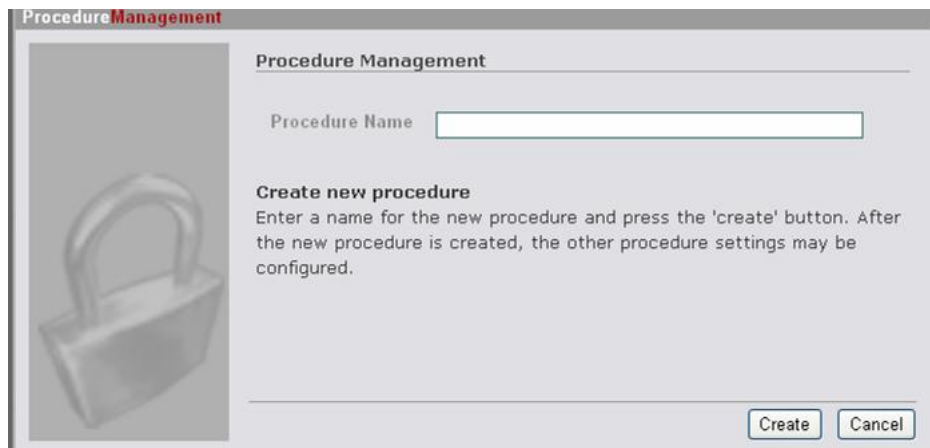
In the description, this could contain the directions “In Windows, press Ctrl, Alt + Del at the same time then choose ‘Change password’”.

## Creating your procedures

To access the Procedures menu, click on [Procedures](#). You will now see the following list of standard procedures:



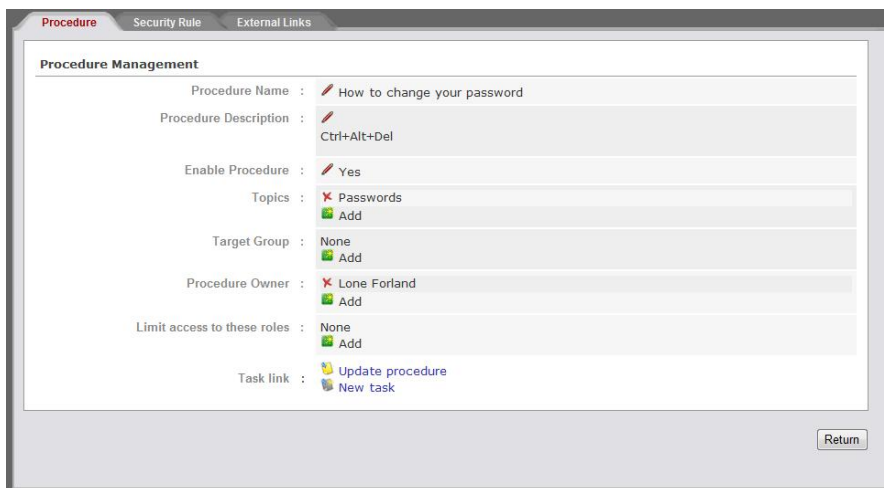
You can use an existing procedure by clicking on [Add procedure from library](#) or create your own by clicking on [New procedure](#). If you want to create your own procedure, you must start by giving it a name.



Once you have written the name of the procedure you wish to set up, click on **Create**.


You have now created a new procedure title which will appear in the list of existing procedures.

Whether you wish to edit your new procedure an existing one, from this point on, the process is the same.




The screen shown below is the same whether you have chosen to edit your own or an existing procedure.


As a rule, the **Procedure** tab will be screen you see first. Here, you can edit the following:


**Procedure Name** – Click on  to change the name


**Procedure Description** – Enter a description of the procedure here.

**Enable Procedure** – Here, you can choose whether or not you want the procedure to be active and to figure in the policy. (To start with, all policies are active).

**Topics** – The procedure can be allocated to one or more topics by clicking on , selecting the desired topic, and clicking on **OK**.

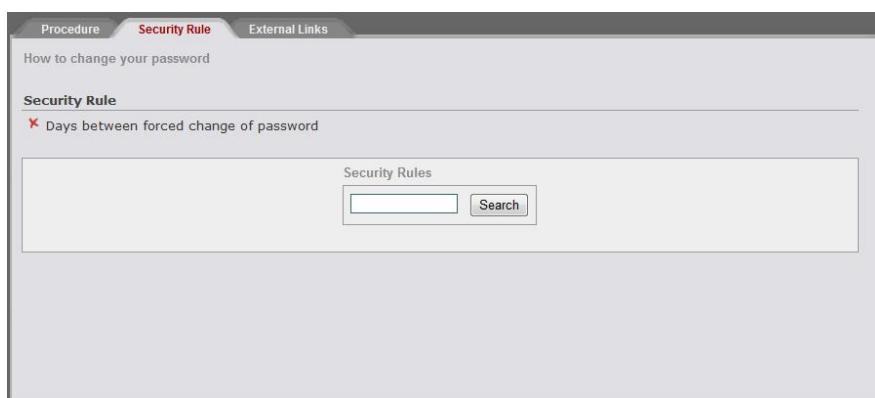
**Target Group** – The procedure can be allocated to one or more specific target group by clicking on , selecting the desired group, and clicking on **OK**. In the standard set up, you can choose between 3 groups: End user, IT Administrator, and Management.

**Procedure Owner** – This function allows you to link a specific user to the procedure. This user will then be responsible for ensuring that the procedure is carried out correctly. Click on . Now you can search for a user using his or her ID, name, or e-mail. Your search will cover all registered SecureAware users. Once selected, click on **OK**.

**Limit access to these roles** – This function allows you to limit access to view procedure to certain groups (for example, Risk-assessment users). Click on , and select the group from the drop-down menu. Click **OK** to complete.

Once you have edited these variables, you can move on to the other tabs, or click on **Return** to go back to the Procedures main menu.

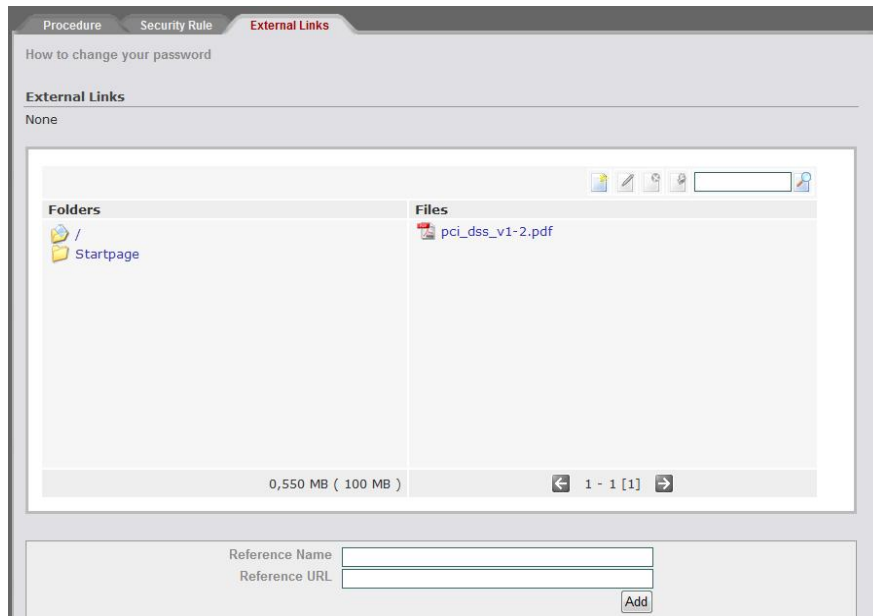
## Linking procedures to rules





Procedures can be linked to specific rules. By clicking on the **Security Rule** tab, you will be able to search for the rule that you want to link the procedure to.

## External Links

The **External Links** tab allows you to link to external documents. A link to such material will be created as an integral part of the chosen procedure.



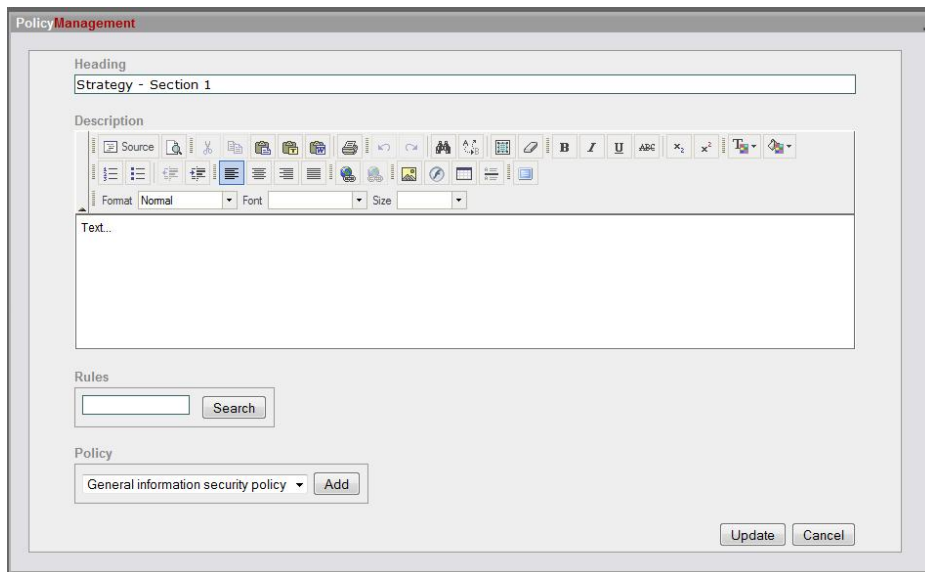
Select a document in the document database or type the name of the reference source in the **Reference Name** box. Write this name as you want it to appear in the final company policy PDF. Edit or delete an existing name using  and  respectively.

You can link to different sections of your company's electronic infrastructure, including http/https, ftp and directly to file-sharing systems.

To save your changes, click on **Update**. You will now return to the Procedure main menu.

# Strategy

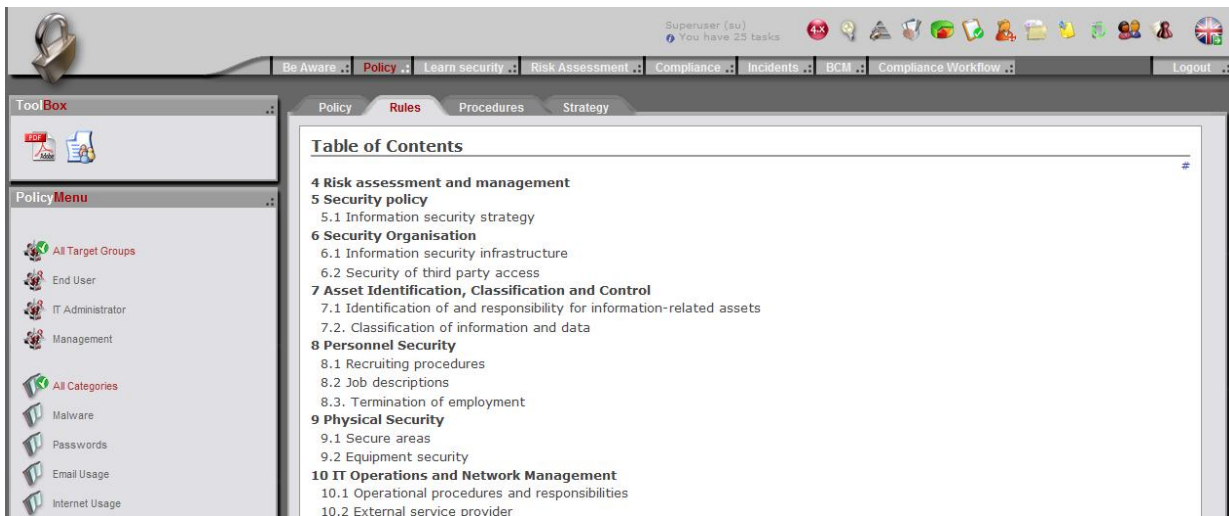
To start with, this part of the policy is empty. Editing this part of the policy is done in the same way as the Policy part (see chapter: Policy).





At the bottom of the screen, you can create links to both rules and policies. Remember to click **Update** to save entries and changes.

# How do the end users see the policy?

When end users log into SecureAware and click on the Policy tab, they will be presented with the active Policy. The tabs are used to navigate between the various policy sections.



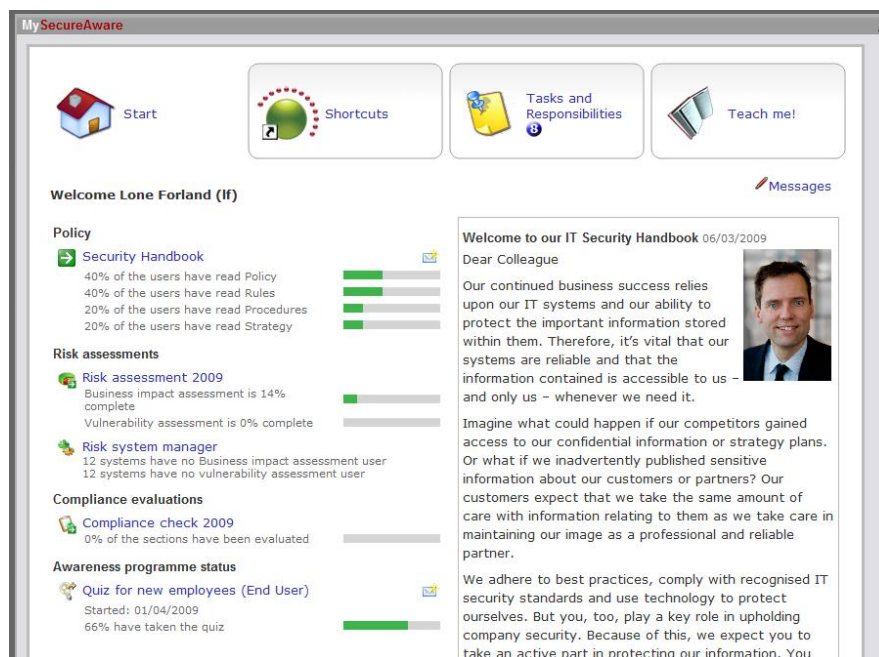
Shown above, is the top tier of policy rules. If the user is listed under a specific target group, he or she will only be presented with rules relevant to this specific group. By clicking on a topic on the left, user will be shown these topic-specific rules.

Scrolling to the bottom of the page, the user will be able to register that he or she has read this policy section by clicking on the  icon. Super Users can view a report over this register by clicking on . The date shows the most recent date a user has read the specific policy section.

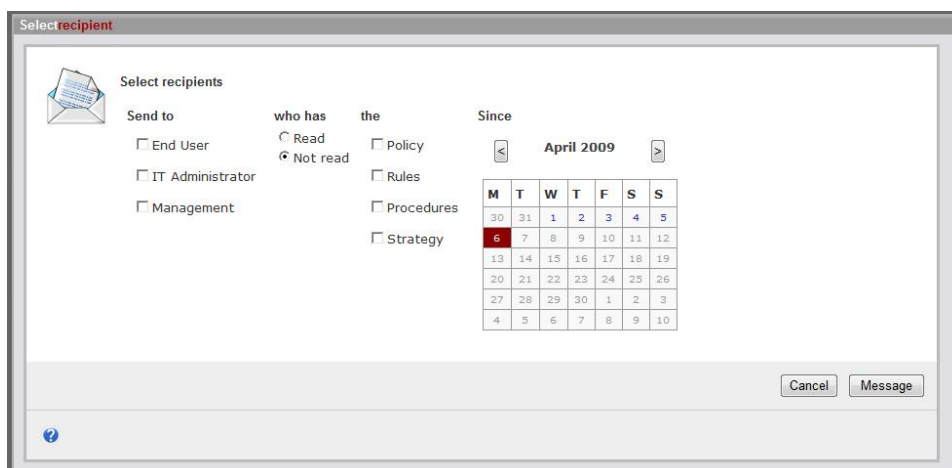
## Who has read the policy

Users	Policy	Rules	Procedures	Principle
Sarah Willis	22/12/2008	22/12/2008	22/12/2008	22/12/2008
Michael Khan	22/12/2008	22/12/2008		
John Smith	22/12/2008		22/12/2008	22/12/2008
Superuser	22/12/2008		22/12/2008	

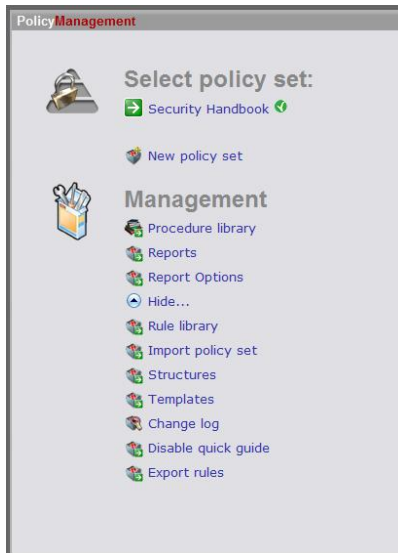
You can see how many users have read specific sections of the policy on My SecureAware (the start page). To send reminders or similar messages to users, click on the mail icon and then select the specific users you wish to contact.




You could choose to send a reminder to those who have or those who have not read any part of the policy set recently, or you could restrict your reminder to any target group or groups. Click on **Message**, write your message, and click **Send**.




# Policy Management





To the bottom left of the main Policy Management menu, you will find a **Management** menu. This menu allows you to manage your policies in much more detail and contains shortcuts which make it easier to submit and edit different elements of your policy.


Click on  **More options...** to fold down and extend this menu.


 **Procedure library** – This menu option allows you to view all procedures, including those which are not actively incorporated in any policy. Clicking here lets you create and edit procedures.


 **Reports** – View complete or specific sections of your policy in PDF or RTF format.


 **Report Options** – Create a new type of report or edit existing ones. PLEASE NOTE! If you have a fourth level in your policy and you want this to show in the full report, you will have to manually add this section to the report.


 **Rule library** – The standard SecureAware program comes with 384 security rules (or sub-menus) which form the basis of the various standards incorporated into the program. (These sub-menus are dealt with in more detail in the next section).


 **Import policy set** – This menu option allows you to import a policy into SecureAware, for instance, a policy from another portal. The program's import function supports all \*.saf (SecureAware File) formatted files. Note: it isn't advisable to use this system as a back up – instead, use the Backup/Restore procedure in the SecureAware System Administrator.

 **Structures** – By clicking here you can access the Secure Category Management menu. This menu allows you to manage the layout you want to use in your security policy. A more in-depth explanation of this is described in the ‘Policy Layouts’ chapter.


 **Templates** – This function allows you to create policies from scratch. You choose the layout using the Policy Layout function (see above). A more in-depth description is given in the ‘Policy Templates’ chapter.


 **Change Log** – All policy changes are registered here. You can view all changes to any given policy within a specific timeframe. You can also generate a PDF file which lists the changes as well as displays the person responsible for carrying them out.

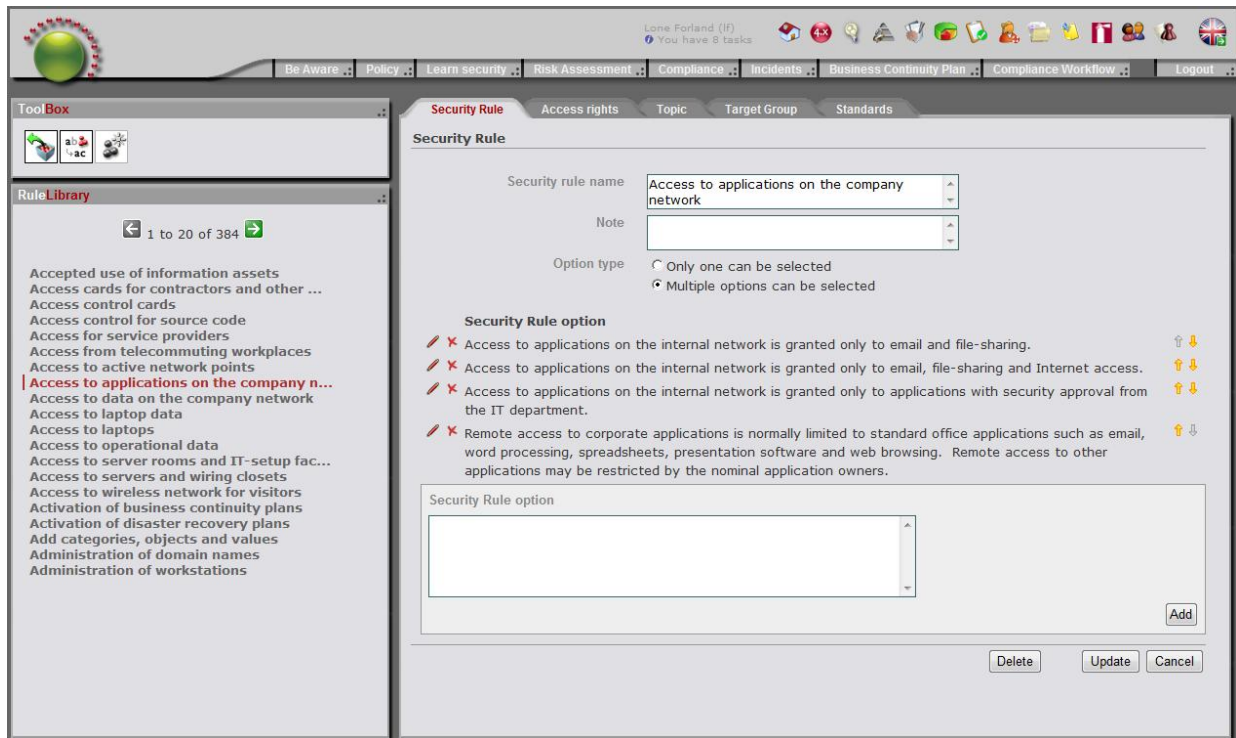
 **Disable quick guide** – Go directly to the main Policy Manager menu each time you start the Policy module

 **Export rules** – Lets you export the policy set.

## The Rule Library

As mentioned, by clicking on  **Rule Library** you are able to manage the rules in SecureAware. The standard program comes with 384 preinstalled rules, but you can add as many others as you require, as well as edit the existing ones.




To start creating your own rules, click on the icon .

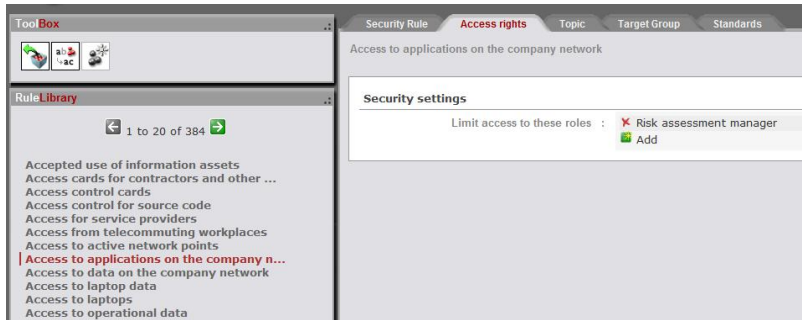



You can name, provide a description of, and add options to your rule. Click on **Create** once done. Now the rule will be shown on the left of your screen in the list of other rules.

Whether you wish to alter one of your own, or one of the existing standard rules, the procedure is the same. By clicking on the rule name in the left-hand menu, the selected rule will appear in the editing screen. You can now carry out the editing you require.

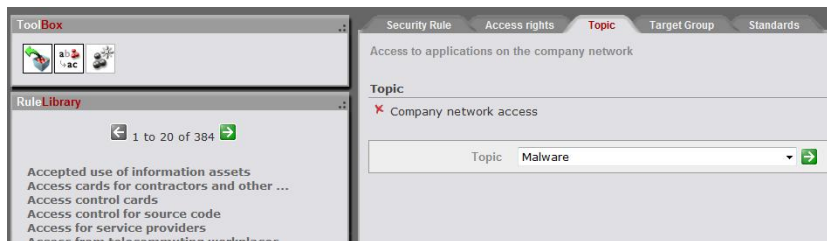
The **Security Rule** tab allows you to alter the rule name and add any notes. **Option type** allows you to choose whether end users can select single or multiple options (rules) in a test. The **Security Rule option** box lets you add options. This option can be selected (or deselected) as a rule listed in your security policy (and will be presented to or hidden from an end user in a test).

The individual options can also be deleted , edited,  or rearranged . Remember to click on the Update button whenever you have made any changes. **Important!** If you choose to edit the option, you must click on both update buttons to save your changes.



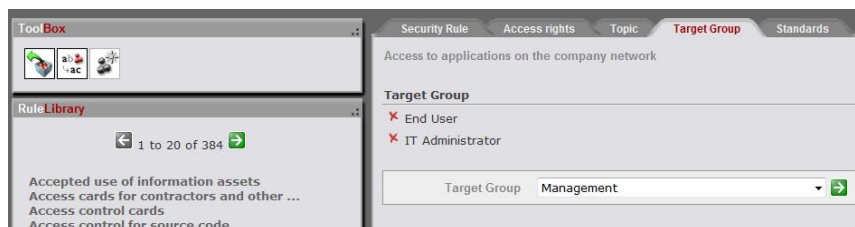
The **Access Rights** tab allows you to limit viewing access to the selected security rule. Click on  **Add** and a drop-down menu will now appear. Select the groups who you want to be able to see this rule when

viewing the security policy. By selecting the default value 'None', the rule will be subject to no restrictions.



The **Topic** tab allows you to select which topic category the security rule will be listed under. If, at a later date, you choose to run an awareness

campaign dealing with this particular topic, the selected rule will be shown as a test option in the relating quiz.




The **Target Group** tab lets you define which target group or groups will be presented with the rule. The selected groups will be

tested in this in an awareness campaign.



The **Standards** tab is useful if you want to allocate a certain security standard to the selected rule. Select the required standard and click

on . Now, you can select the specific section of the chosen standard with which you wish the rule to comply.


## Policy Structures

As mentioned, SecureAware has several predefined structures. These are split into categories and subcategories and some follow the same structure as particular standards – e.g. ISO17799. Because these standard structures may not necessarily be 100% suitable for your company, SecureAware allows you to edit the layout to best meet your individual security requirements.





The 4 predefined standard layouts are:


- **SecureAware 2:** A layout suitable for use with SecureAware version 2.x.x.
- **SecureAware 3:** A layout suitable for use with SecureAware version 3.x.x.
- **DS484:2005 layout:** A layout that reflects the DS484 standard.
- **ISO17799:2005 layout:** A layout that reflects the ISO17799 standard.



To create a new layout (or change the name of an existing one), click on  **Create and manage policy layouts**.



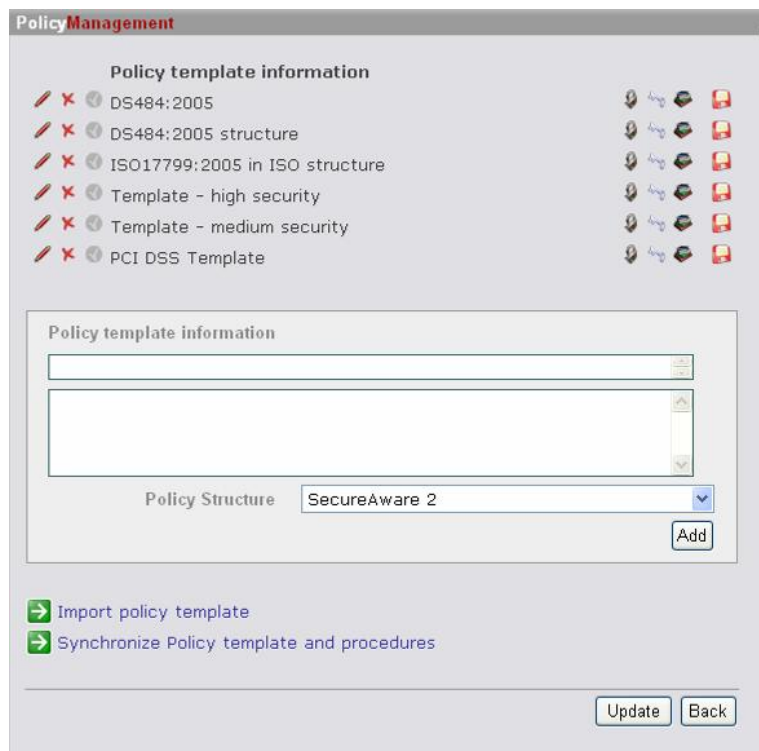
Edit the layout name using . Delete a layout using . Activate/deactivate a layout using  (a green tick shows an active layout). To export a layout from SecureAware, click on .

To create a new layout, start by entering the layout name in the Security Category Layout box and then click on **Add**. To import a layout, click on .

Remember to save any changes you have made by clicking on **Update**.

## Policy Templates




Once you have selected the layout for your new policy, you can set up a template with which you can create your security policy. If you have created your own layout, the template can be used with this. SecureAware comes with a number of standard predefined templates.



Below is a list of the predefined SecureAware templates:

- **DS484:2005:** A complete policy in accordance with the DS484 standard.
- **DS484:2005 in DS layout:** A complete policy in accordance with the DS484 standard set out with the same section-numbering system as listed in the DS policy standard. The matching layouts make it simple for your policy to comply with the necessary criteria of this standard.
- **ISO17799:2005 in ISO layout:** Requirements from ISO17799:2005 listed in the same layout format. Section numbering in this template corresponds to the numbering and order of the ISO standard.
- **Template – high security:** This template provides an excellent starting point if your company requires a relatively high level of security without requiring 100% compliance with ISO17799 or DS484. The layout is based upon these standards but with increased emphasis on user friendliness.

- **Template – medium security:** This template provides a good foundation for creating a policy if your company doesn't require an overly high level of IT security. Although based upon the ISO17799 and DS484 standards, this template is free from the restrictive compliance requirements these standards demand. Particularly suitable for medium-sized manufacturers and smaller service companies.

Click on  to edit the name, and click on  to delete. (Note that completely deleting a template you don't want to use is not always necessary). If you want to export a layout from SecureAware, click on the  icon.

### Creating a new policy template


If you want to create your own policy template, enter your template name in the Policy template information box. In the larger box under this, you can add a brief description of your new template. (This description will be shown when you create a new policy in the Policy Management main menu). To select the desired layout for your template, use the **Policy structure** drop-down menu.

Now click on **Add**, followed by **Update** to save your changes.



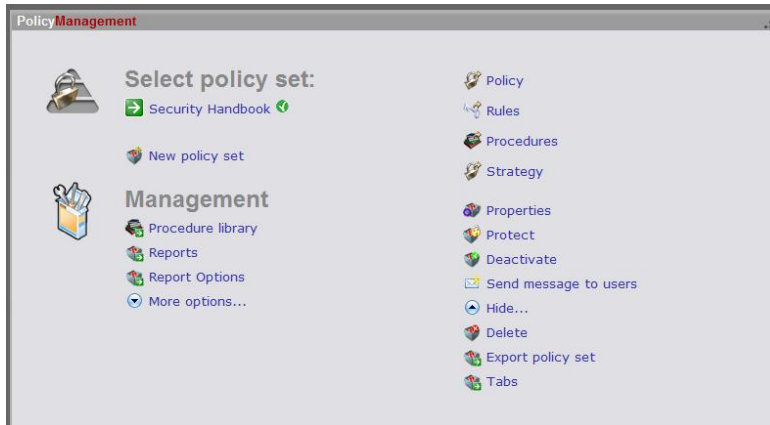
The screenshot shows a web form titled "Policy template information". It contains a text input field with "NewTemplate" entered, a larger text area with "Description of NewTemplate", and a dropdown menu for "Policy Structure" set to "SecureAware 2". There is an "Add" button to the right of the dropdown. Below the form are two links: "Import policy template" and "Synchronize Policy template and procedures", both with green arrow icons. At the bottom right are "Update" and "Back" buttons.


Import a template by using  **Import policy template**.


If you click on  **Synchronize Policy template and procedures**, you can attach a procedure to your template. By synchronizing, the selected procedures will be attached to the template you are creating. (Note: this will not affect exiting policies based upon this template.)

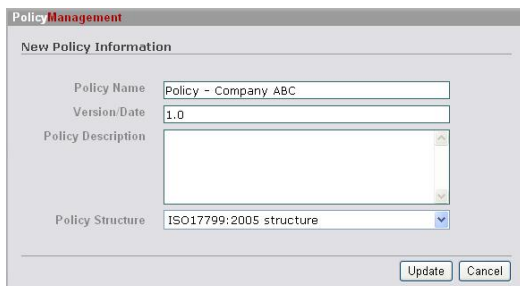
Important! Following any changes, always click on **Add** followed by **Update** to save.


## Managing the company's policy






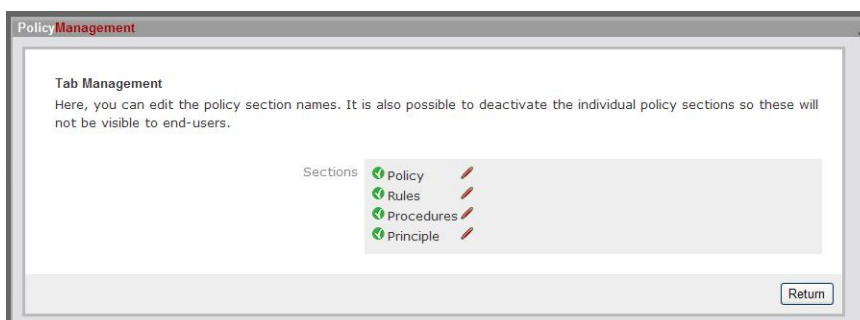
On the right-hand side of the Policy Management main menu you will find an advanced management menu. Clicking on  **More options...** expands the menu.

The individual menu items relate only to the policy that is active at that time. Any editing will therefore affect this policy only. (An active policy is marked with a ).




By clicking on  **Properties** you can rename a policy, add or change a version number or date, and add a brief description. Clicking on this menu item also allows you to alter the structure upon which your policy is based.

You can delete a policy by clicking on  **Delete**. However, once deleted, a policy is lost forever so choosing  **Deactivate** is often more prudent. Reactivate a dormant policy by marking it on the left of the screen and clicking on  **Activate**.

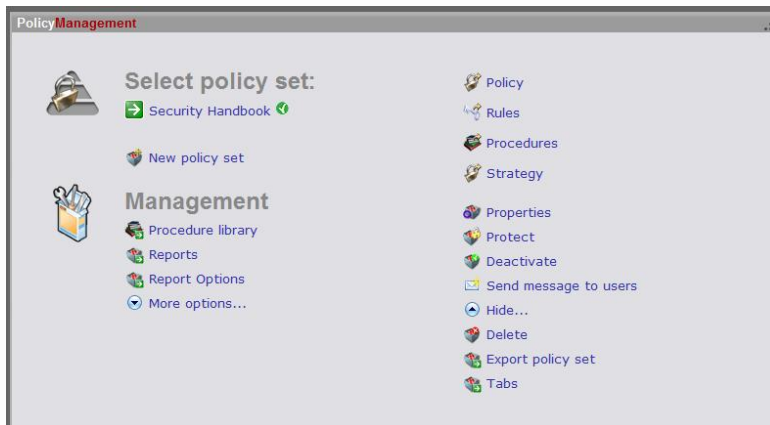


If you wish to alter the default SecureAware terms "Policy", "Rules", "Procedures" and "Strategy" to terms more suitable for your company, click on **Tabs**.

You can now enter your own names and, additionally, you can determine which levels your end users will be shown.

If you use a SecureAware portal solution in particular, exporting policies between portals can be of particular use. To do this, click on  **Export policy set**. Remember, exporting a policy is not intended as a back-up function. Read more about this in SecureAware's back-up of database procedure.

## Copying a policy (import and export)



You may often find it useful to make a copy of a policy so that you can edit one version whilst leaving the original version active and accessible to users. This requires exporting the policy then importing it once you have edited it as required. To do this, activate the desired policy, fold down the

**More options...** menu, and then click on **Export policy set**. This policy will now be exported as a 'saf' file (SecureAware File) and can be placed wherever you choose.



Now click on **Import Policy set** and find the location of the required file. Once you have imported and uploaded the file you will see it listed alongside the other policies. It will have the same name as the original policy but will include the time and date of the import, as shown below. You can rename the policy by clicking on **Properties**. You can now choose to edit this policy set leaving the original policy active until you are ready to replace it with your edited version.

# SecureAware's logging facilities

Logging facilities have been incorporated within SecureAware to allow you to trace and document all editing carried out in the Policy module and to document any errors in the system at large.

To do this, logging facilities are embedded in both the Policy module and in the system administrator's management functions.

Additionally, several SecureAware modules include information linking data to specific users. Here, the normal data processed is traced and documented by the system and not by a specific log

## **Policy module maintenance log**

The report logs and shows the date, user name and action taken in relation to rules, options and procedures.

To access the report, click **More options...** on the left hand side and then click on **Change Log**. Then select the policy and period you wish your log to show.

To view an error log, you must be logged on as a System Administrator. See the System Administrator manual for more.

# Contact Information

- Further information is available by contacting Neupart

## Europe

Neupart A/S  
Hollandsvej 12  
2800 Lyngby  
Denmark  
Tel +45 7025 8030  
Fax +45 7025 8031

## North America

United States  
Neupart Inc.  
2553 Crescent St  
Ferndale, WA 98248  
Tel. 360-820-2545  
Fax 360-392-6078

Neupart GmbH  
Kaiserwerther Strasse 115  
40880 Ratingen/Düsseldorf  
Germany:  
Tel. +49 (0) 2102/4209-26  
Fax +49 (0) 2102/42062

Copyright © 2006 Neupart A/S. All rights reserved.

The author of this documentation is Neupart A/S. All information herein including text and graphics belongs to Neupart A/S unless stated otherwise and is protected by copyright laws in Denmark and international agreements.

Permission to quote this documentation in its entire form or partly is given under the premises that no changes are made and that information about this copyright is clearly stated on all copies. No material may be copied or distributed without explicit approval of Neupart A/S. Neupart A/S preserves the right to - at any time and without warning - make changes and/or improvements in the products mentioned.

Names of other companies and their products are or can be registered trademarks or trademarks that belong to their owners. Neupart and SecureAware logo and the name "SecureAware" are trademarks belonging to Neupart A/S. The documentation is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the documentation or the use or other dealings in the documentation. The documentation including graphics could contain inaccuracies or typographic errors. Furthermore there are no guarantees regarding results achieved by using this information.

All rights not explicitly mentioned herein are preserved.