

# Symantec Data Loss Prevention

## EU and UK Solution Pack

### Configured Policies

Policy Group	Policy Name	Policy Description
UK and International Regulatory Enforcement	Caldicott Report	<p>The Caldicott Report (December 1997) was a review commissioned by the Chief Medical Officer to make recommendations to improve the way the National Health Service handles and protects patient information. The Caldicott Committee was set up to review the confidentiality and flows of data throughout the NHS for purposes other than direct care, medical research, or where there is a statutory requirement for information. Its recommendations are now being put into practice throughout the NHS and the Health Protection Agency.</p> <p>***Requires EDM as best practice and to minimize false positives***</p>
	Human Rights Act 1998	<p>The Human Rights Act, 1998, allows UK citizens to assert their rights under the European Convention on Human Rights in UK courts and tribunals, and states that “so far as possible to do so, legislation must be read and given effect in a way which is compatible with convention rights.” This policy enforces Article 8 by ensuring the private lives of British citizens stay private.</p> <p>***Requires EDM as best practice and to minimize false positives***</p>
Employee Data Protection	UK Drivers License Numbers	<p>This policy detects UK Drivers License Numbers using the official specification of the UK Government Standards of the UK Cabinet Office.</p>
	UK National Insurance Numbers	<p>The UK National Insurance Number is a reference number issued to a person by the Department for Work and Pensions and Inland Revenue (DWP/IR) for participants in the National Insurance Scheme.</p>

Policy Group	Policy Name	Policy Description
<b>Confidential Data Protection</b>	Competitor Communications	This policy detects communications with specific company competitors. Customize with addresses of specific competitors. ***Requires input of customized competitor addresses***
	Confidential Documents	This policy detects company-confidential documents at risk of exposure.
	Encrypted Data	This policy detects the use of encryption by a variety of methods including S/MIME, PGP, GPG, and file password protection.
	Financial Information	This policy detects financial data and information.
	Mergers and Acquisitions	This policy is used to detect discussion of sensitive Mergers and Acquisitions activity. Customize the keywords list by adding internal terms for M&A activity. ***Requires input of customized keywords***
	Resumes	This policy detects active job searches.
	Source Code	This policy detects various types of source code leaving the network.

## Available Response Rules

Rule	Action	Condition
<b>Automated Responses – Blocking Messages</b>		
Block SMTP Email *ONLY available with Network Prevent (Email)*	Block SMTP Message Set Status to Escalated	Severity is High
Block Web Communication *ONLY available with Network Prevent (Web)*	Block HTTP/HTTPS Request Set Status to Escalated	Protocol is HTTP, SSL, IM:MSN, IM:AIM, IM: Yahoo, FTP, NNTP Severity is High
Remove Web Content *ONLY available with Network Prevent (Web)*	Remove HTTP/HTTPS Web Content Set Status to Escalated	When Protocol is any of HTTP, SSL, IM:MSN, IM:AIM, IM: Yahoo, FTP, NNTP Severity is High
<b>Automated Responses – Quarantining Emails</b>		
Quarantine SMTP Email *ONLY available with Network Prevent (Email)*	Modify SMTP Message Change Header 1 name to "X-CFilter-Quarantine" and the value to "Yes". Set Status to Escalated	Severity is Medium
<b>Automated Responses – Endpoint Actions</b>		
Block Copy to Removable Media *ONLY available with Endpoint Prevent*	Endpoint: Block Set Status to Escalated	Severity is High

Rule	Action	Condition
Notify End User *ONLY available with Endpoint Prevent*	Endpoint: Notify	Severity is Medium
<b>Automated Responses – Protecting Files</b>		
Quarantine File, from network file share *ONLY available with Network Protect*	Protect: Quarantine File Set Status to Escalated	Severity is High
Copy File on network file share *ONLY available with Network Protect*	Protect: Copy File	Severity is Medium
<b>Automated Responses - Resolutions</b>		
Notify and Resolve	Send Email Notification (to sender) Set Status to Resolved Set Resolution Attribute: Automatically Resolved	Severity is Low
Resolve with No Action	Set Status to Resolved Set Resolution Attribute: Automatically Resolved	Severity is Info
<b>Automated Responses - Notification</b>		
Notify of Critical Incident	Send Email Notification (to manager) Send Email Notification (to sender) Set Status to Escalated	Severity is High
<b>Smart Responses - Notifications</b>		
Notify Sender	Send Email Notification (to sender)	Manually Executed
Notify Manager	Send Email Notification (to manager)	Manually Executed
<b>Smart Responses - Escalations</b>		
Escalate for Investigation	Set Status to Investigation	Manually Executed
<b>Smart Responses - Dismissals</b>		
Dismiss, Bus. Process Issue	Set Status to Dismissed Set Dismissal Reason Attribute: Bus. Process Issue	Manually Executed **Strongly recommend adding comment to incident indicating business process and actions to correct**
Dismiss, False Positive	Set Status to Dismissed Set Dismissal Reason Attribute: False Positive	Manually Executed
<b>Smart Responses - Resolutions</b>		
Resolve, Business Issue	Set Status to Resolved Set Resolution Attribute: Business Issue	Manually Executed **Strongly recommend adding comment to incident indicating next steps**

Rule	Action	Condition
Resolve, Education Issue	Set Status to Resolved Set Resolution Attribute: Education Issue	Manually Executed **Strongly recommend adding comment to incident indicating educational next steps.**
Resolve, Employee Oversight	Set Status to Resolved Set Resolution Attribute: Employee Oversight	Manually Executed **Recommend adding comment to incident describing oversight.**
Resolve, One-time Event	Set Status to Resolved Set Resolution Attribute: One-time Event	Manually Executed
Resolve, Reply Oversight	Set Status to Resolved Set Resolution Attribute: Reply Oversight	Manually Executed
Quarantine Files		User must set severity to High to trigger rule.

## Configured Roles and Reports

Role	Description	Reports
<b>ISR</b>  Access=new status, all policies	InfoSec Responder role. First level of incident response for specific policies. Find broken business processes. Fan-out to extended remediation team.  Role Permissions: <ul style="list-style-type: none"> <li>• Views incidents/reports</li> <li>• Remediates incidents</li> <li>• Looks up attributes</li> <li>• Deletes incidents</li> <li>• No access to sender/recipient identity details</li> <li>• Views or Edits some custom attributes</li> </ul>	Incident Queue (for all policies except for HIPAA and Resumes, new status). 1 for each for Network, Endpoint, and Data at Rest.
<b>ISM</b>  Access=all statuses; all policies except for Resumes	InfoSec Manager role. Second level of incident response. Manage escalated incidents within InfoSec team.  Role Permissions: <ul style="list-style-type: none"> <li>• Views incidents/reports</li> <li>• Remediates incidents</li> <li>• Looks up attributes</li> <li>• Deletes incidents</li> <li>• Edits all custom attributes</li> <li>• Authors all policies and policy groups</li> <li>• Authors response rules</li> </ul>	Incident Queue (for Competitor Communications, Financial Information, Source Code, Mergers and Acquisitions, Confidential Documents, Encrypted Data policies; Escalated status). 1 for each for Network, Endpoint, and Data at Rest.

Role	Description	Reports
<b>Audit</b>  Access=all statuses, all policies	Auditor role. Ensure compliance regulations are being met. Develop strategies for risk reduction at Business Unit level. View incident trends and risk scorecards. Role Permissions: <ul style="list-style-type: none"> <li>• Views incidents/reports</li> <li>• Remediates incidents</li> <li>• Looks up attributes</li> <li>• Deletes incidents</li> <li>• Edits all custom attributes</li> </ul>	Incident Queue (for Caldicott Report, Human Rights Act 1998, UK Drivers License Numbers, UK National Insurance Numbers policies' Escalated status). 1 for each for Network, Endpoint, and Data at Rest.
<b>HRM</b>  Access=all statuses, all policies	HR Manager role. HR/Employee Relations Officers. Respond to incidents that lead to employee termination. Role Permissions: <ul style="list-style-type: none"> <li>• Views incidents/reports</li> <li>• Remediates incidents</li> <li>• Looks up attributes</li> <li>• Deletes incidents</li> <li>• Edits all custom attributes</li> </ul>	Incident Queue (for HIPAA and Resume policies, all statuses). 1 for each for Network, Endpoint, and Data at Rest.
<b>Report</b>  Access=all statuses, all policies	Reporting and Policy Authoring role. Provides single role for demonstration and Risk Assessment oversight Role Permissions: <ul style="list-style-type: none"> <li>• Views incidents/reports</li> <li>• Remediates incidents</li> <li>• No access to incident details</li> <li>• Authors all policies, policy groups, and response rules</li> <li>• No Discover scan control</li> </ul>	None
<b>Investigator</b>  Access=all statuses, all policies	Investigator or Legal role. Researches further details of incidents. Includes incidents forwarded to forensics. Investigates specific employees. Role Permissions: <ul style="list-style-type: none"> <li>• Views incidents/reports</li> <li>• Remediates incidents</li> <li>• Looks up attributes</li> <li>• Deletes incidents</li> <li>• Edits all custom attributes</li> </ul>	Incident Queue (for all policies; Investigation status). 1 for each for Network, Endpoint, and Data at Rest.

Role	Description	Reports
<b>Exec</b>  Access=all statuses, all policies	Executive role. Ensures data risk reduction at macro level. Reviews risk trends and performance metrics. Reviews risk dashboards.  Role Permissions: <ul style="list-style-type: none"> <li>• Views incidents/reports</li> <li>• Remediates incidents</li> <li>• Looks up attributes</li> <li>• Deletes incidents</li> <li>• Views all custom attributes</li> <li>• No Discover scan control</li> </ul>	None
<b>Sys Admin</b>  Access=all statuses, all policies	System Administrator role. To encourage users to use roles other than Administrator.  Role Permissions: <ul style="list-style-type: none"> <li>• User administration</li> <li>• System administration</li> <li>• Views incidents/reports</li> <li>• No access to incident details</li> <li>• No access to shared or custom attributes</li> <li>• No Discover scan control</li> </ul>	None

## Configured Users

User	Role	Description
Admin	System Administrator (standard system role)	Provides technical system administration for Symantec Data Loss Prevention.
User 1	All Roles except System Admin	Provides ability to create shared reports across other roles without different logins.  **Virtual Role- does not need to be assigned to a specific person.**

## Attributes Enabled

Status Attributes	Status Group	Status
	Open	New, Escalated, Investigation
	Closed	Resolved
	Dismissed	Dismissed

Custom Attributes	Resolution*	Dismissal Reason*	Assigned to	Business Unit
	Employee Code	First Name	Last Name	Phone
	Sender Email	Manager Last Name	Manager First Name	Manager Phone
	Manager Email	Region	Country	Postal Code

\*The values for these custom attributes should be pre-determined.

## Additional Protocols Enabled

Protocols	TCP: Telnet	TCP: SSH	TCP: SSL	TCP: Pop3
	TCP: IRC	TCP: EDonkey	TCP: Gnutella	TCP: BitTorrent
	TCP: Napster	TCP: DirectConnect	TCP: FastTrack	

© 2011 Symantec, Inc. All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Symantec. While every precaution has been taken in the preparation of this document, Symantec assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice. Symantec and all Symantec product names are the trademarks or registered trademarks of Symantec, Inc. All other company and product names are the trademarks or registered trademarks of their respective owners.

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043

<http://www.symantec.com>