proofpoint.

LEVEL TWO
DIGITAL RISK: SOCIAL PATROL CONQUERING CONTENT POLICIES

FORMAT
Web-Based Training (WBT)

DURATION
40 minutes

INTENDED AUDIENCE
System Administrator, IT, Security or Compliance Manager

PREREQUISITES
Fundamentals of Social Patrol

REGISTRATION
Contact training@proofpoint.com for registration information

The course incorporates best practices, step-by-step processes and short videos for content policies including key concepts, built-in policies, content categories, classifiers actions, how to create a new, edit, duplicate to customize, revert and delete a policy, access, filter and export an audit log.

COURSE OUTLINE

Lesson 1: Definition, Permissions and Access
Understand content policies, required system permissions and how to access content policies in Social Patrol

Lesson 2: Key Terms in a "Flash"
Understand key terms associated with content policies including Brand (Outbound) Policy, Brand Social Media Accounts, Built-In Policies, Classifiers, Classifiers Actions, Commenter (Inbound) Policy, Dynamic/Interactive Content, Individual Social Media Accounts, Scan-Only, Social Selling Media Accounts and Static Content

Lesson 3: Built-in Policies and Classifiers
Understand built-in policies, benefits, classifiers and brand versus commenter content

Lesson 4: Content Classifier Actions
Describes the five actions taken on a content policy classifier: none, log, notify, hide and/or delete

Lesson 5: Informational Categorizations
Describes when the "Notify" action is selected

Lesson 6: Customize a Content Policy: Two Options
Describes how to customize a content policy using the create new or by duplicating a built-in policy

Lesson 7: Edit a Content Policy
Describes how to edit a current content policy category classifier action

Lesson 8: Delete a Content Policy
Describes how to delete a customized policy

Lesson 9: Revert a Content Policy
Describes how to undo clear policy classifier actions

Lesson 10: Audit Policy Changes Log
Describes how to access and review audit log changes by date and user and exporting a log to a CSV file