jobscience

Compliance User Guide

Jobscience, Winter '18

Last Updated: February 10, 2018

TABLE OF CONTENTS

About This Guide

This guide is provided for anyone interested in learning:

- The detailed capabilities of the Compliance App.
- The process for developing, circulating, and enforcing compliance policies.
- How to set up your own compliance program within the App.

Overview

The Compliance App is a tool that enables you to develop, document, and enforce policies to protect your business. Policies can include data protection, information security, human resources, and any other policies your business manages.

We recommend that you consult experts and define policies that are appropriate for your business. Compliance does not define or offer advice regarding your actual policies. It merely provides the structure required to manage the policies your company has defined.

This document uses concrete examples from the Jobscience InfoSec policy, but only as an example. Nothing in these examples is warranted for accuracy or legality.

The Getting Started Step-by-Step section describes the steps required for setting up a compliance program and using the system to manage your monitoring and enforcement of the policies.

Participants

The Compliance App is designed for use by a hierarchy of internal users that define, review, and circulate your policies to internal employees. You should designate a team within your business to review, approve, and disseminate your policies. These team members should access Compliance as full users of Salesforce. They should be assigned Permission Sets for one or more of the following Roles:

- Policy Author
- Policy Publisher
- Compliance Manager
- Compliance Auditor

Internal employees are expected to review policies, acknowledge reading them, and periodically review them as part of the compliance process. We recommend that employees who need to be aware of your policies, but are not active in the management of the policy, access the information via a defined Employee Community. The primary purpose of the community is to make the employee aware of the policies and get them to self-acknowledge the policy system and policies. The Employee Permission Set is used with these community users to ensure they have the proper access.

The Compliance App is designed to enable third parties to make requests of your business to provide data, remove information, and request that data be updated. In our system, we expect external constituents to access the system via a Consumer Community site. The Third Party permission set is used with these community users to ensure proper access.

Data Model

Policies

Policy objects are the heart of the system and the hub for all of the other objects. A Policy can be a single concept such as:

> *"All computers used by employees must have updated Anti-virus software installed before accessing any Company Confidential information."*

Policies can also be grouped together by relating them to a parent Policy, which is more abstract such as:

> *"Jobscience Information Security Policy"*

These high level policies may include hundreds of individual policies in a full hierarchy. There is no limit to the number of levels supported, but we recommend that you keep it relatively flat; ideally corresponding to the way your current written policies are structured.

For example, the **Jobscience Information Security Policy** is structured like the ISO Standard 27002:2013 Sections five through 18. Following this structure, there is a top-level policy to represent the entire InfoSec Policy and 13 Policies that represent the major sections of the ISO Policy, such as **Network Security Management**.

Each of these 13 policies has two layers below that. When written out, the policies appear to be a table of contents. Using the example of the ISO Policy, one branch of the tree is shown below with the level numbers in parenthesis:

Jobscience Information Security Policy (1)

- Network Security Management (2)
  - Systems and Network Access Controls (3)
    - Access Controls (4)
    - Accounts (4)
    - Regular Review of Access Controls (4)
    - Remote Access Authorization (4)
    - Revocation of Access (4)

The benefit of this structure is that a single policy at the bottom level can usually be written in a single paragraph and easily understood by the employees of the company. For example, **Revocation of Access**:

> *"Jobscience will revoke Personnel's access to physical locations, systems, and applications that contain or process Customer Data within twenty-four (24) hours of the cessation of such Personnel's need to access the system(s) or application(s)."*

The Policy object in Compliance and its page layouts enable you to capture the information associated with a policy and place it into an appropriate structure for Approvals, Revision control, and all of the other phases of the policy's life cycle.
Jobscience provides a set of stages that explicitly tracks the lifecycle of a policy:

- Drafted
- Reviewed
- Circulated
- Approved
- Published
- Archived

Your organization can define their own custom stages, if necessary, and replace the standard sets that come with the product.
In addition to the Policy object, there are six additional objects that enable you to manage the processes associated with your policies:

- Model Terms
- Requests
- Violations
- Actions
- Audits
- Logs

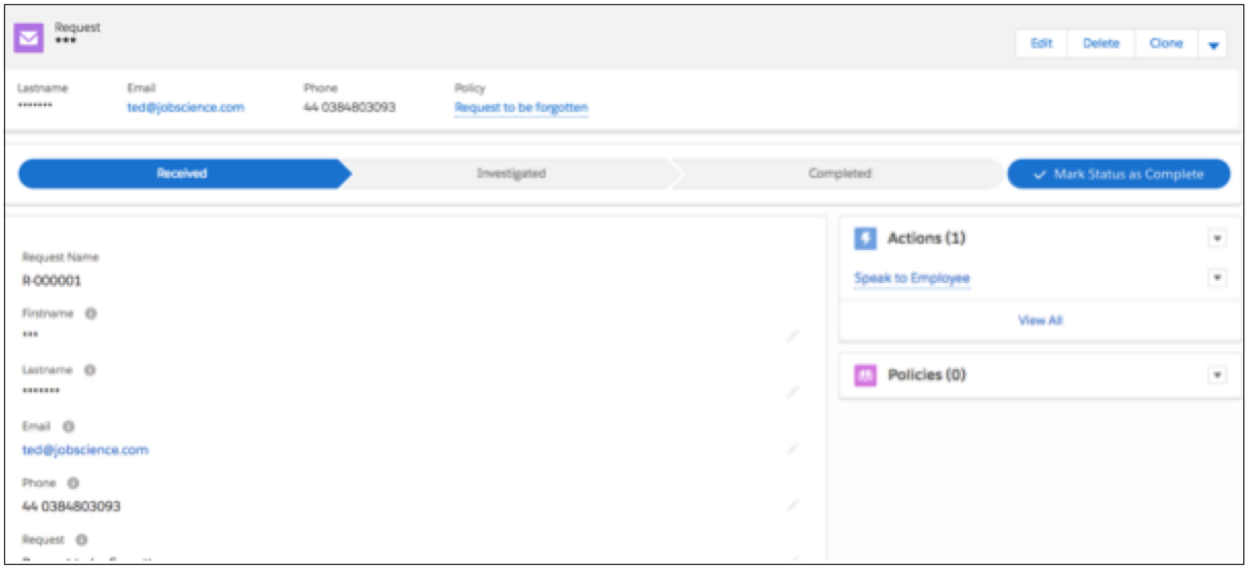
Each object is explained below.

Model Terms

Model Terms provide language that should be included in contracts and the statement of policy on your public documents and websites.
We strongly recommend that you consult legal advice from a compliance consultant for definitions of your model terms.

Requests

Requests are a record of parties asking for action to be taken to enforce a policy, for example a request to be removed from a mailing list. The key concept of a Request is to demonstrate to a regulator or auditor that you have a means for processing requests per your established policies. We recommend that you work with your legal counsel and/or consultants to develop request processes that ensure compliance with the prevailing regulations.
Like Policies, Requests have a lifecycle as well.
When a request is made, it is marked *Received* and can be moved through *Investigated* and then marked *Completed*. The request is stored in an encrypted manner and is linked to actions and policies. A Request is a series of stages that can be updated by your administrator.



Request
***

Lastname	Email	Phone	Policy
*******	ted@jobscience.com	44 0384803093	Request to be forgotten

Request Name
R-000001

Firstname
***

Lastname
****

Email
ted@jobscience.com

Phone
44 0384803093

Request

Actions (1)
Speak to Employee

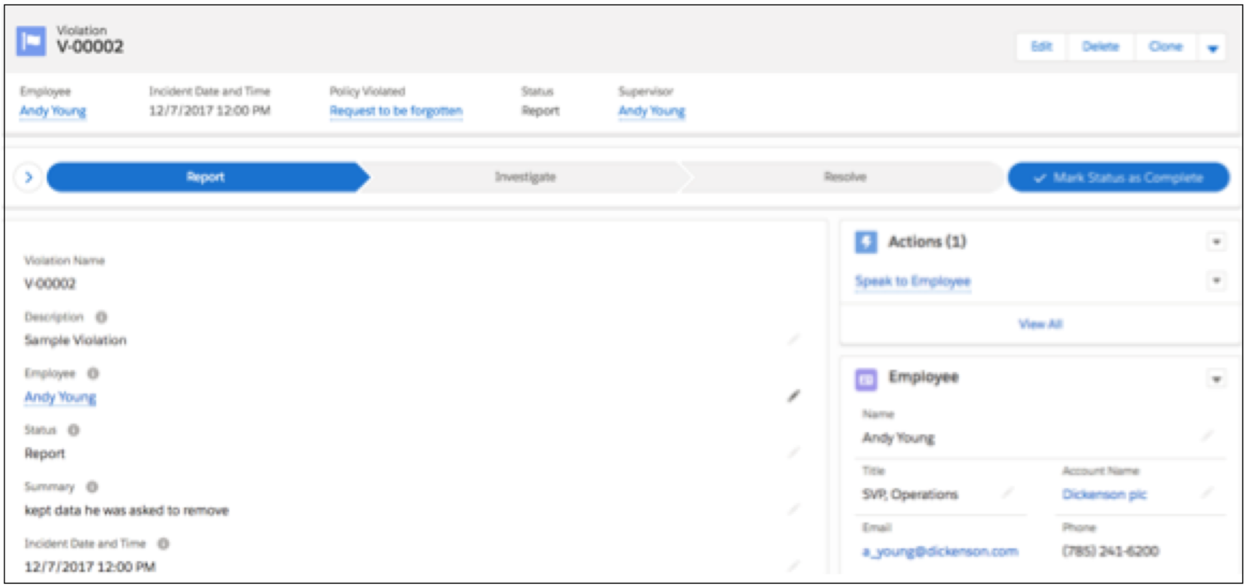
Policies (0)

Since the Request is a standard Jobscience object, it can be used to trigger workflows or business processes when created or updated to a new stage. A workflow or business process can generate an Action to record the steps that are required to respond to the request.

Violations

Violations are a memorialization of a policy violation. The violation is linked to the policy and identifies what has occurred and who is responsible for a policy breach. Violations should be recorded and corrected per the guidelines provided by your legal counsel and/or consultants.

The key concept of a Violation is that it provides you with a basis for demonstrating to a regulator or auditor that you have a means for enforcing and correcting failures in your organization and to show that you have done so for any specific breach.
Violations should be followed up with an investigation and action plan to correct the violation and be closed out after the action has corrected the problem. Violations are created manually, but a workflow or business process can generate an Action to record the steps required to respond to the breach.



Violation
V-00002

Employee	Incident Date and Time	Policy Violated	Status	Supervisor
Andy Young	12/7/2017 12:00 PM	Request to be forgotten	Report	Andy Young

Violation Name
V-00002

Description
Sample Violation

Employee
Andy Young

Status
Report

Summary
kept data he was asked to remove

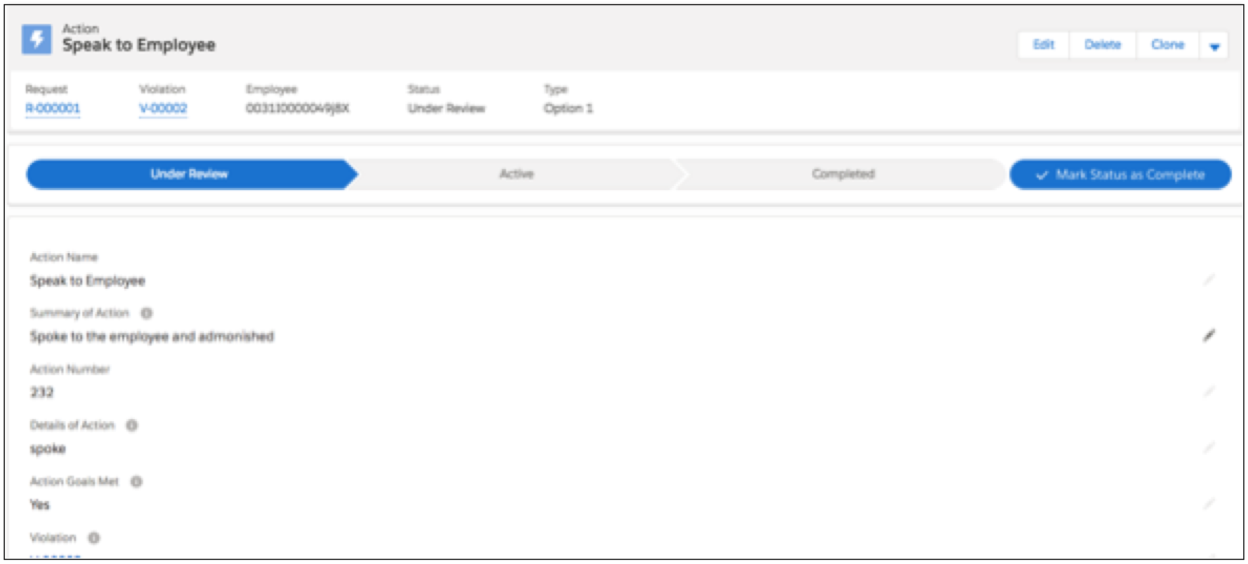
Incident Date and Time
12/7/2017 12:00 PM

Actions (1)
Speak to Employee

Employee
Name
Andy Young
Title
SVP, Operations
Account Name
Dickenson plc
Email
a_young@dickenson.com
Phone
(785) 241-6200

Actions

Actions are a record that your organization has done something to address a Violation or a Request per the guidelines provided by your legal counsel and/or consultants. The key concept of an Action is to demonstrate to a regulator or auditor that you have a means for recording actions per your established policies and that you have taken the appropriate action for a given Request or Violation.



Action
Speak to Employee

Request: R-000001
Violation: V-00002
Employee: 003110000049j8X
Status: Under Review
Type: Option 1

Action Name
Speak to Employee

Summary of Action
Spoke to the employee and admonished

Action Number
232

Details of Action
spoke

Action Goals Met
Yes

Violation

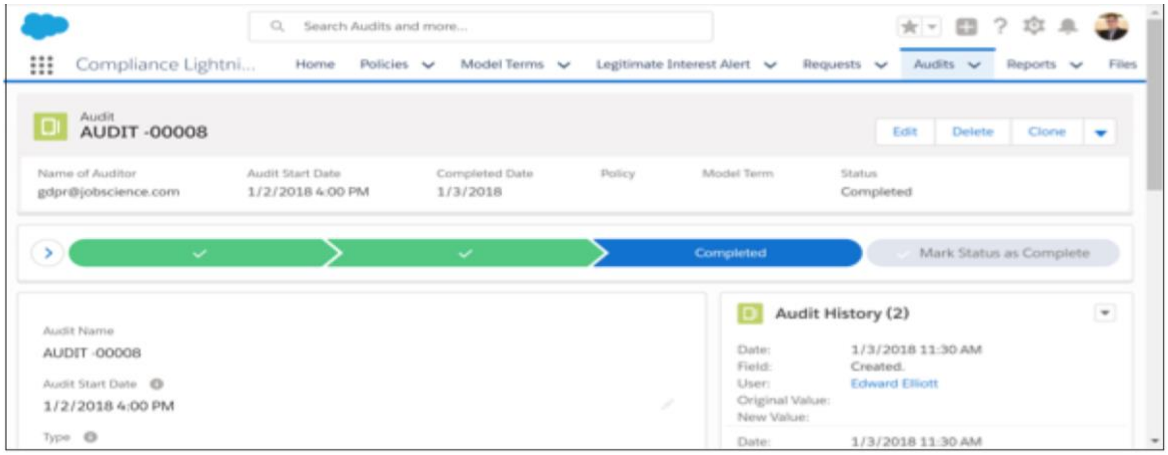
Actions are linked to Requests and Violations and reflect the follow up activity to resolve any open issues regarding a policy.
Actions have a defined lifecycle as well. The default stages include:

- Under Review
- Active
- Completed

Administrators can modify stages to fit the process of your organization.

Audits

Audits are a record that someone has reviewed and/or acknowledged a policy. Audits enable a company to show that it has an active process for educating its workforce regarding defined policies and reviewing the policies to ensure they are actively reviewed.
Many policies will require that employees read and acknowledge certain policies when they are hired and throughout their employment on a regular basis. Audit records are designed to record this event.



Audit
AUDIT -00008

Name of Auditor: gdpr@jobscience.com
Audit Start Date: 1/2/2018 4:00 PM
Completed Date: 1/3/2018
Policy
Model Term
Status: Completed

Audit Name
AUDIT -00008

Audit Start Date
1/2/2018 4:00 PM

Type

Audit History (2)

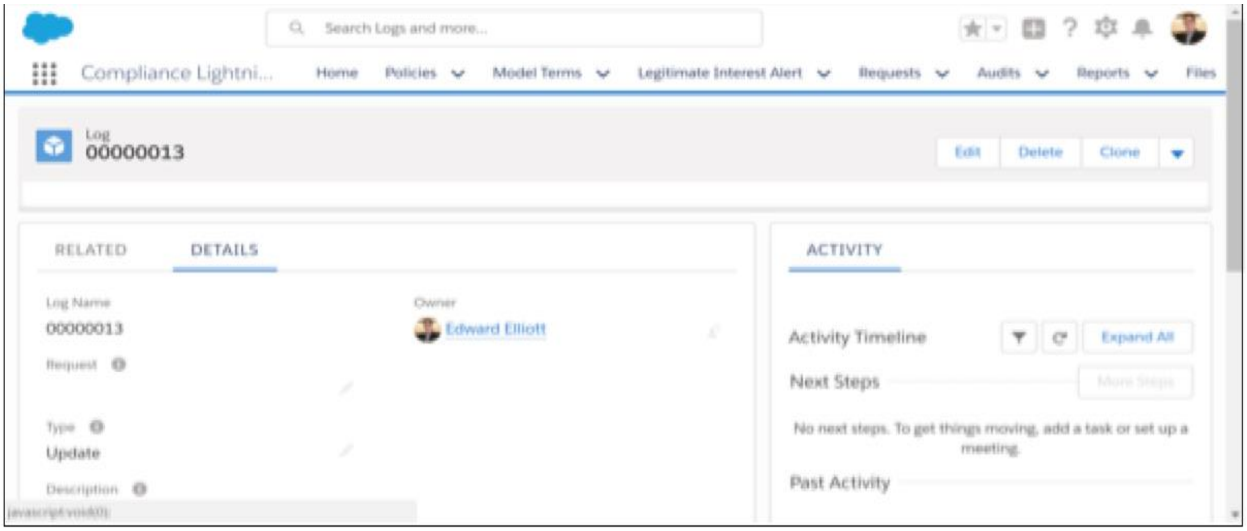
Date: 1/3/2018 11:30 AM
Field: Created.
User: Edward Elliott
Original Value:
New Value:

Date: 1/3/2018 11:30 AM

Logs

Log objects are used to record all compliance-related activities for archive and reporting purposes. They are created using Process Builder Processes any time a Request, Violation, Audit, or Action record is created or modified. The permissions for Log records are limited to Create and Read for everyone in the org so that the logs may not be modified or deleted. This provides a safeguard against unauthorized changes or deletion of the other records. A Violation or Request record may be altered or deleted by a user for example, but a log of this record's creation and any subsequent edits will be stored in the Logs.

In addition, Request, Violation, and Action records use separate objects from one another to facilitate the business process automation. This makes it difficult to produce a report that combines them all in simple chronological order. Logs eliminate this challenge.



Log
00000013

Log Name
00000013

Owner
Edward Elliott

Request

Type
Update

Description

No next steps. To get things moving, add a task or set up a meeting.

Legitimate Interest

One important class of Compliance Policies is related to the concept of Legitimate Interest. For direct marketers, this will generally involve the proper support for opting out of emails and support for the right to be forgotten.

For long-term relationships though, it is often important to know the last time your organization had any interaction with a contact in your database. Interaction in this case means:

- Sending an Email or SMS
- Making a Phone call
- Sending an Invitation for an event

These are all indications of continuing interest in the contact. The problem arises when there is **no** interaction for extended periods of time. Can you really say you have a legitimate interest in a contact if you have not even emailed them in more than two years?

Applications are usually designed to take action when something happens. This creates a challenge when you want to take action when nothing happens. For example, it is easy to detect no activity for 90 days in Salesforce, but then how do you continue to remind the team to resolve this issue after the initial alert?

The Compliance App provides an object called Legitimate Interest Alert (LIA), which represents a potential challenge to Legitimate Interest. These can be created through any process you want to define, but we provide one method out of the box to detect the inactivity use case mentioned above.

This process is triggered based on the "Last Activity" date on the Contact record. The default time delay is 90 days, but the admin can change it with a setting. Last Activity is reset any time a task or event is created on this Contact. So as long as users are generating activity around this Contact and combining it with a Task or Activity, the trigger will never fire.

If after 90 days there has been no activity, the trigger will fire and create a Legitimate Interest Alert record. The creation of this LIA record can then generate additional actions. The Default Action is to create a Task, assigned to the Owner of the neglected contact, which drives them to review this contact and either interact with them if appropriate, or archive the record if that is the process your company wants to follow. You can set a due date on that task which will generate an overdue task as a reminder. You could create a Business Process that sends out an email to the Contact Owner once a Legitimate Interest Alert record is created.

Data Privacy Support in Salesforce

With the release of Spring 2018, Salesforce now provides standard support for tracking Data Privacy Preferences. These preferences are an important part of the process required to comply with:

- General Data Protection Regulation (GDPR), European Union
- Gramm-Leach-Bliley Act (GLB Act), United States
- Canada’s Anti-Spam Law (CASL)

The New Data Privacy records are used to track and store customers’ preferences for:

- Collecting, storing, and sharing their personal data.
- Packaging their personal data so they can take ownership of it.
- Deleting records and personal data related to them.
- Solicitation of products and services.
- Tracking their geolocation and web activity.

Within Jobscience you can associate each Data Privacy Record with a Contact to track their consent. Even though Data Privacy Records let you track and store certain data privacy preferences, it is up to you to determine how to honor them.

Fields in Data Privacy Records

Field	Description
Birth Date	The Customer’s birthdate.
Block Geolocation Tracking	Preference not to track geolocation on mobile devices.
Don’t Process	Preference to not process personal data, which can include collecting, storing, and sharing personal data.
Don’t Profile	Preference to not process data for predicting personal attributes, such as interests, behavior, and location.
Don’t Solicit	Preference to not solicit products and services.
Don’t Track	Preference to not track web activity.
Export Individual’s Data	Preference to export personal data for delivery to the individual.
First Name	The customer’s first name, as it appears in the data privacy record. Maximum 40 characters.
Forget This Individual	Preference to delete records and personal data related to this individual.
Individual’s Age	Indication for whether the individual is considered to be a minor.
Last Name	The customer’s last name as it appears in the data privacy record. Maximum 80 characters.
Name (Full Name)	The customer’s first, middle, and last names as they appear in the data privacy record.
OK to Store PII Data	Indication that you can store personally identifiable information outside

Elsewhere	of their legislation area. For example, you could store an EU citizen's personal data in the US.
Salutation	The title for addressing the customer, for example, Mr., Ms., or Dr. Admins set the values available. Maximum 40 characters.
Suffix	The suffix in the customer's name, as it appears in the data privacy record. Maximum 40 characters.

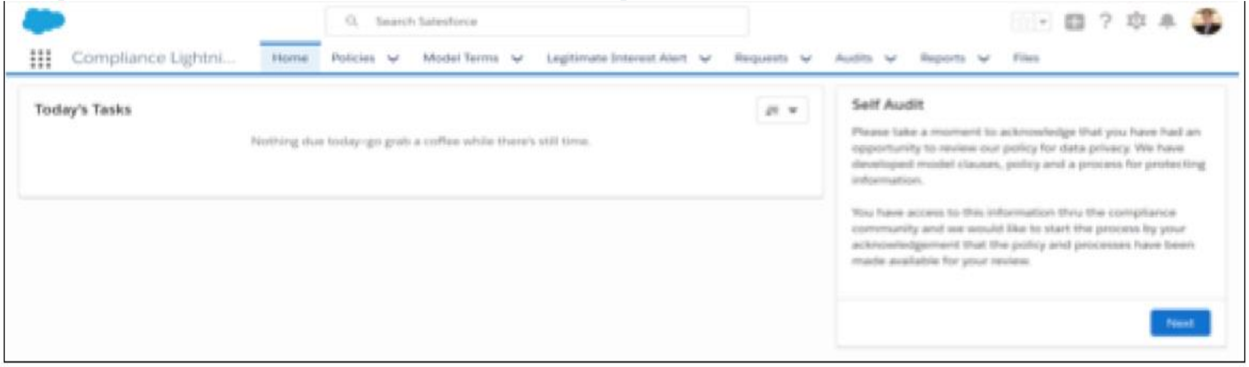
For a complete reference on support for Data Privacy in Salesforce, refer to the following Community Article in the Trailblazer Community: Store Customer's Data Privacy Preferences.

Getting Started Step-by-Step

This section provides step-by-step instructions for getting your first policy published and associated processes launched:

- Step 1: Define and Provision Participants
- Step 2: Review and Enable
- Step 3: Define Policies
- Step 4: Define Model Terms
- Step 5: Create your Employee Community
- Step 6: Create your Consumer Community

Step 1: Define and Provision Participants



Today's Tasks

Nothing due today-go grab a coffee while there's still time.

Self Audit

Please take a moment to acknowledge that you have had an opportunity to review our policy for data privacy. We have developed model clauses, policy and a process for protecting information.

You have access to this information thru the compliance community and we would like to start the process by your acknowledgement that the policy and processes have been made available for your review.

As covered in the Overview, you should designate a team within your business to review, approve, and disseminate your policies. These team members should access the Compliance App as full users of Salesforce. Provision them with accounts if they do not already have one and assign one or more of the following four permission sets as appropriate for their role:

- Policy Author
- Policy Publisher
- Compliance Manager
- Compliance Auditor

Permission Sets are additive and multiple sets may be awarded to a single user.
Give the Policy Author permissions to anyone who will author Policies.
In general, Authors do not publish their own policies. Identify the approvers in the organization and give them the Policy Publisher Permission Set. If an individual both authors and publishes, they can be awarded both Permission Sets.

A **Compliance Manager** is the role that receives requests and issues violations. The people in that role will also be responsible for reviewing actions and following up on the ones carried out by others.

A **Compliance Auditor** is responsible for ensuring all employees have acknowledged the active policies when they are hired, when policies are updated, and to reconfirm they are still in compliance on a regular basis.

Step 2: Review and Enable Processes

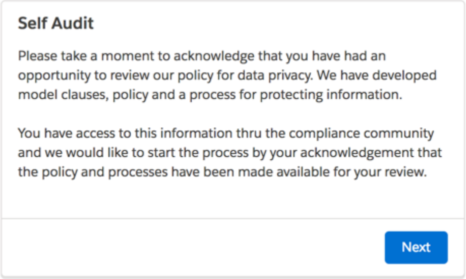
There are several aspects to the built-in automations that should be reviewed before deploying this App.

The first aspect is related to the stages defined for the objects of the package. Policies, for example, use a default set of stages beginning with Drafted, Reviewed, and Circulated. The Compliance team should review the stage values for each of these objects and determine if any changes are required. Stages may be added, removed, or renamed for each object. Note that making changes to these stages may require changes to the associated Business Processes.

Once the stages are confirmed, the team should review and understand the automations defined by the App. These can be grouped by:

- Approval Processes
- Flows
- Process Builder
- Object Triggers

Determine if your organization wants to implement formal Approval Processes for policy review and publication. These processes are very specific to your organization, so none are defined out of the box.



Self Audit

Please take a moment to acknowledge that you have had an opportunity to review our policy for data privacy. We have developed model clauses, policy and a process for protecting information.

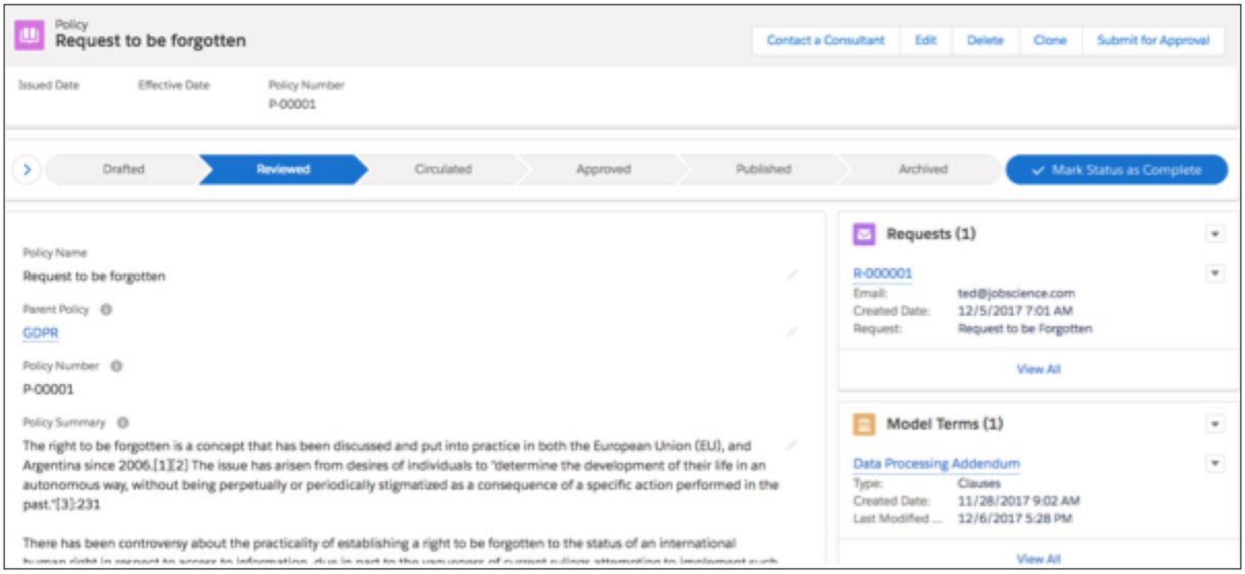
You have access to this information thru the compliance community and we would like to start the process by your acknowledgement that the policy and processes have been made available for your review.

"Self-Audit" is the only Flow defined out of the box. It is responsible for displaying this element on the home page. It is designed to present a list of policies that must be reviewed and acknowledged by the user.

There are several Process Builder Processes that are associated with Logs. This is where the new Log records are created each time a new record is created or a change occurs. Logs are very powerful, but over time will consume storage space. With normal activity, these logs should not grow too large too fast, but over time they may require attention. Determine if the Logging feature is appropriate for your company and if all of the entities should be logged. If the team decides that one or more of the entities are not required in the logs, deactivate the associated Process to prevent logs from being created.

Step 3: Define Policies

You can create a policy by selecting the Policy tab and then clicking the **New** button.



Policy
Request to be forgotten

Issued Date

Effective Date

Policy Number
P-00001

Policy Name
Request to be forgotten

Parent Policy
GDPR

Policy Number
P-00001

Policy Summary
The right to be forgotten is a concept that has been discussed and put into practice in both the European Union (EU), and Argentina since 2006.[1][2] The issue has arisen from desires of individuals to "determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past."[3]:231

There has been controversy about the practicality of establishing a right to be forgotten to the status of an international

Requests (1)

R-000001

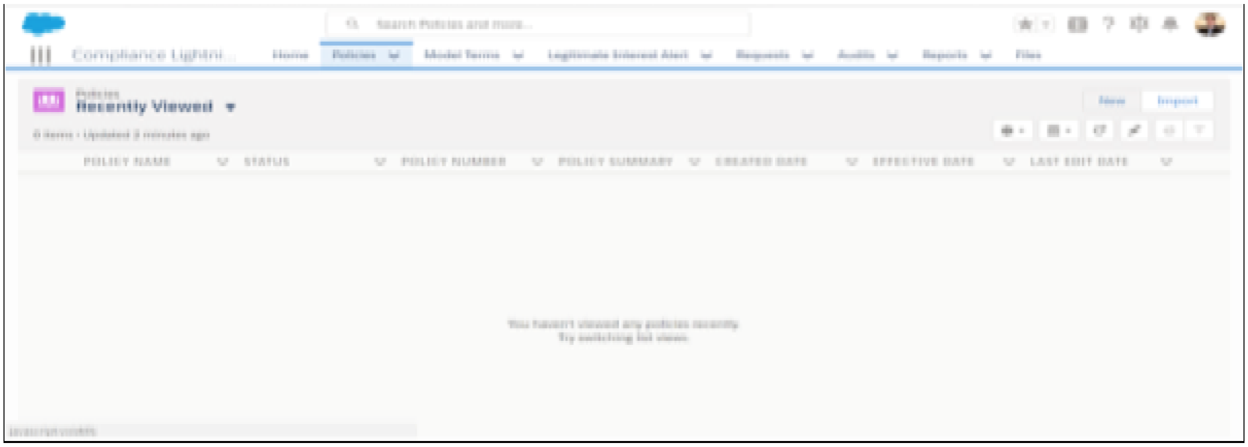
Email:	ted@jobscience.com
Created Date:	12/5/2017 7:01 AM
Request:	Request to be Forgotten

Model Terms (1)

Data Processing Addendum

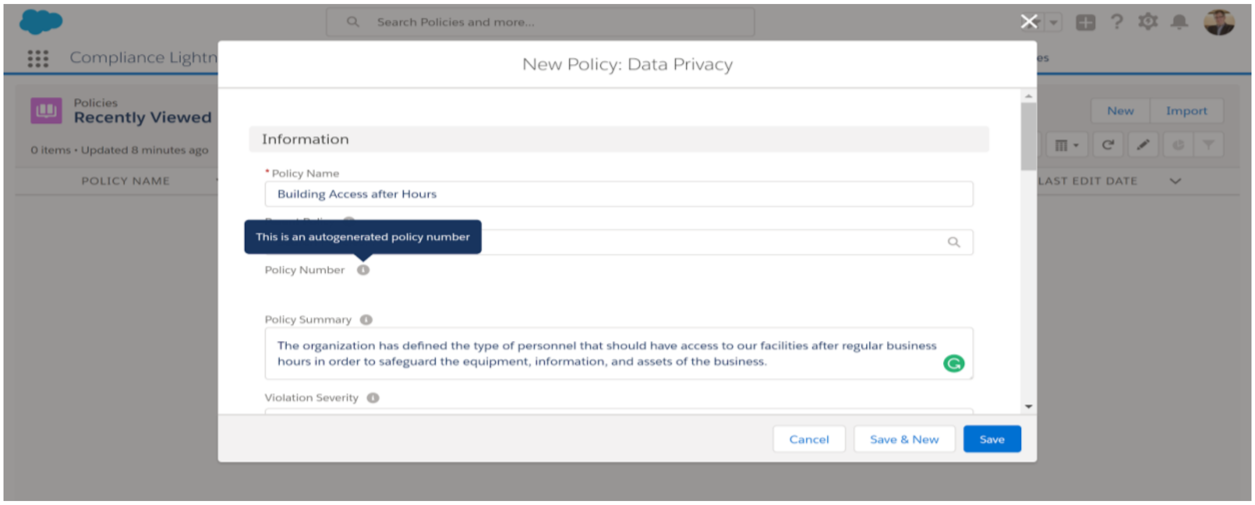
Type:	Clauses
Created Date:	11/28/2017 9:02 AM
Last Modified ...	12/6/2017 5:28 PM

A dialog box displays asking you to complete information about the policy. Take a moment to complete the information fields as fully as possible. Define a Policy Name that easily describes the policy and determine if this policy has a parent policy that it should be attached to. Provide a short summary that describes the policy.



0 items • Updated 3 minutes ago

You haven't viewed any policies recently.
Try switching list views.



0 items • Updated 8 minutes ago

New Policy: Data Privacy

Information

* Policy Name: Building Access after Hours

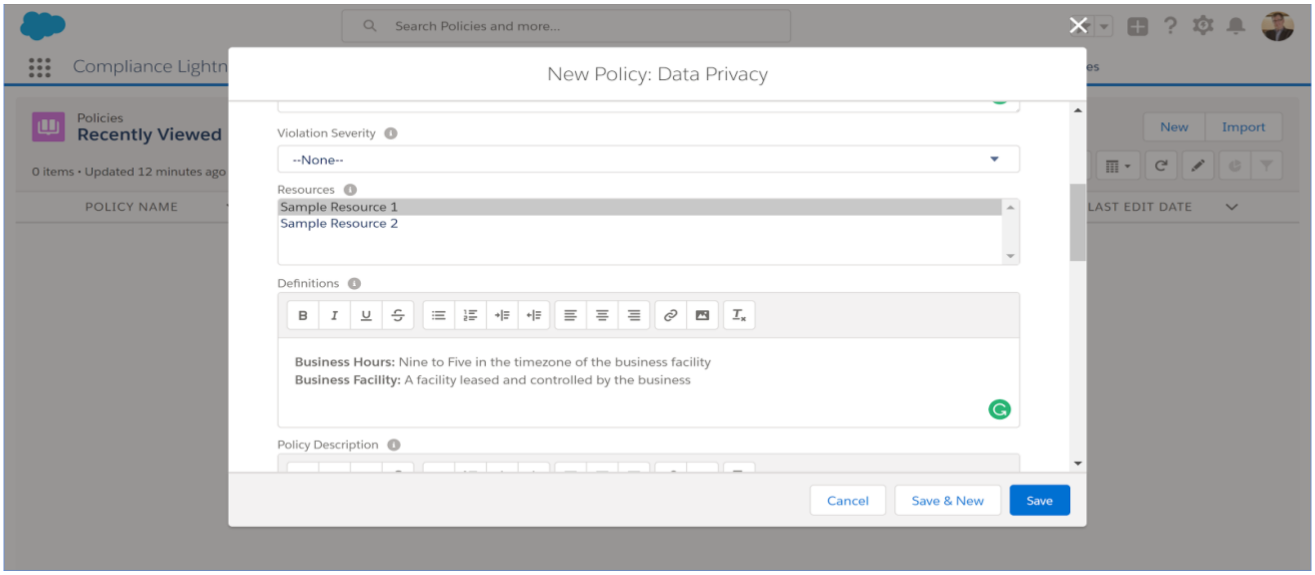
This is an autogenerated policy number

Policy Number

Policy Summary: The organization has defined the type of personnel that should have access to our facilities after regular business hours in order to safeguard the equipment, information, and assets of the business.

Violation Severity

Next, define the severity of a policy violation and define a custom list of resources that should be available to properly enforce and maintain the policy. In order to customize the application, an administrator can go into the Policy object and define the picklist options for resources that match your business. Then you should define any terms used repeatedly in the policy that require a clear definition.



New Policy: Data Privacy

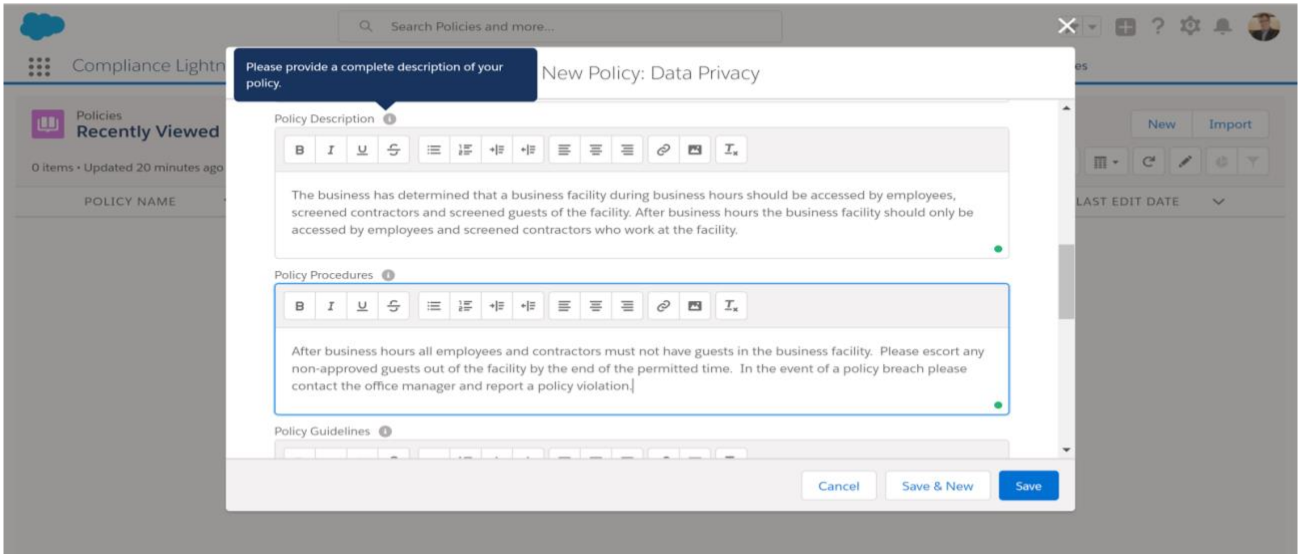
Violation Severity: --None--

Resources: Sample Resource 1, Sample Resource 2

Definitions:

Business Hours: Nine to Five in the timezone of the business facility
Business Facility: A facility leased and controlled by the business

Now take a moment to fully describe the policy and the procedures for the enforcement of the policy. This is important for providing guidance on how to execute the policy.



Please provide a complete description of your policy.

New Policy: Data Privacy

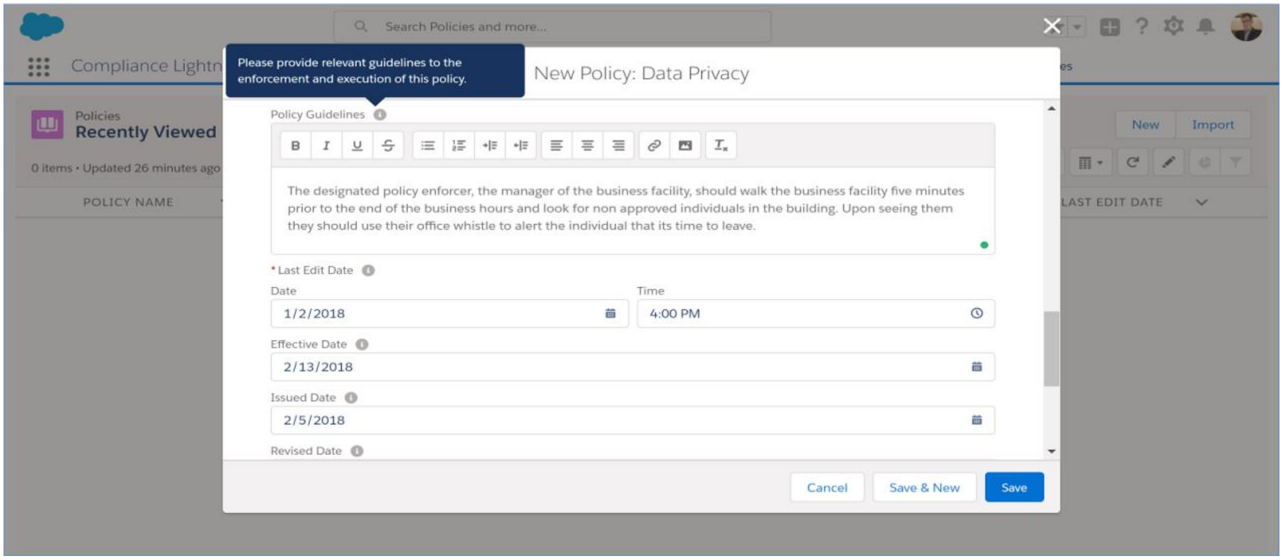
Policy Description:

The business has determined that a business facility during business hours should be accessed by employees, screened contractors and screened guests of the facility. After business hours the business facility should only be accessed by employees and screened contractors who work at the facility.

Policy Procedures:

After business hours all employees and contractors must not have guests in the business facility. Please escort any non-approved guests out of the facility by the end of the permitted time. In the event of a policy breach please contact the office manager and report a policy violation.

Please provide guidelines for the policy in order to assist employees and managers in the proper execution of their duties. Also define when the policy was drafted, effective, and issued into the policy of the business.



Please provide relevant guidelines to the enforcement and execution of this policy.

New Policy: Data Privacy

Policy Guidelines

The designated policy enforcer, the manager of the business facility, should walk the business facility five minutes prior to the end of the business hours and look for non approved individuals in the building. Upon seeing them they should use their office whistle to alert the individual that its time to leave.

*Last Edit Date

Date: 1/2/2018

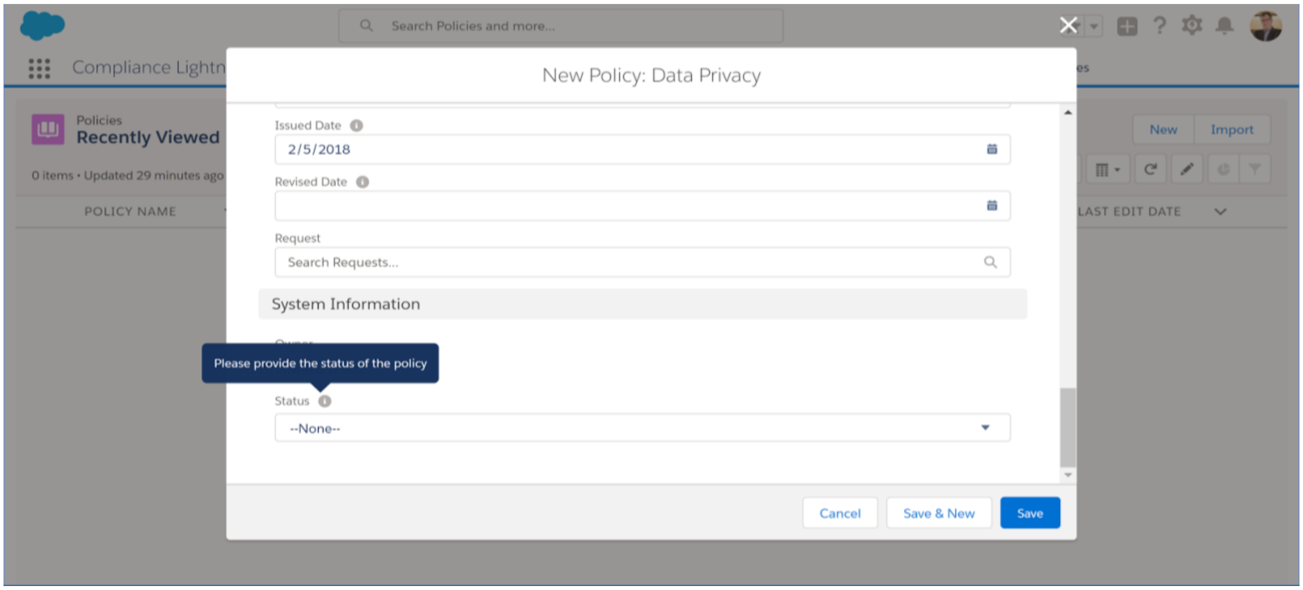
Time: 4:00 PM

Effective Date: 2/13/2018

Issued Date: 2/5/2018

Revised Date

Please indicate if there is a revised date and any request that was the source of the policy creation. The system will designate a policy owner based on the individual who created or entered the information. Depending on your internal approval process there is a set of statuses to apply to the policy to ensure a proper approval and notification process has been followed in the creation of the policy.



New Policy: Data Privacy

Issued Date: 2/5/2018

Revised Date

Request: Search Requests...

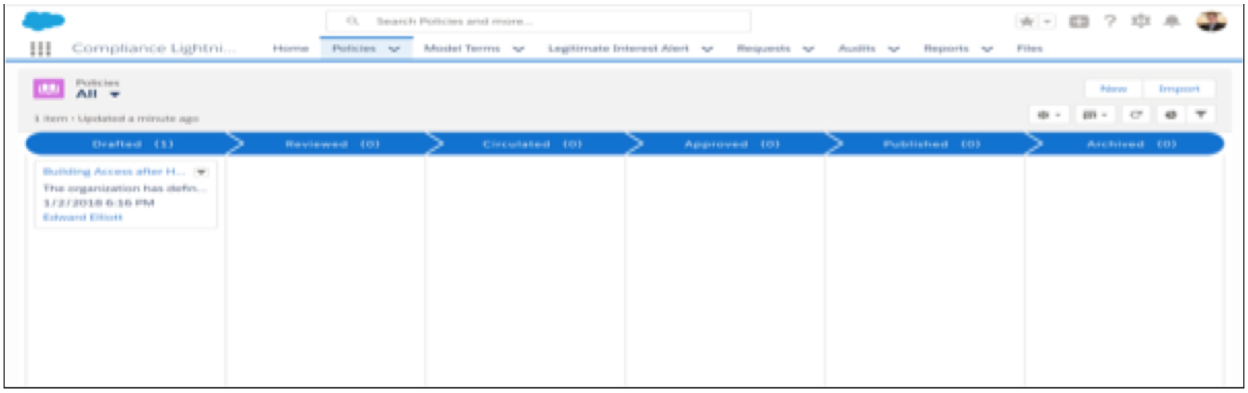
System Information

Owner

Please provide the status of the policy

Status: --None--

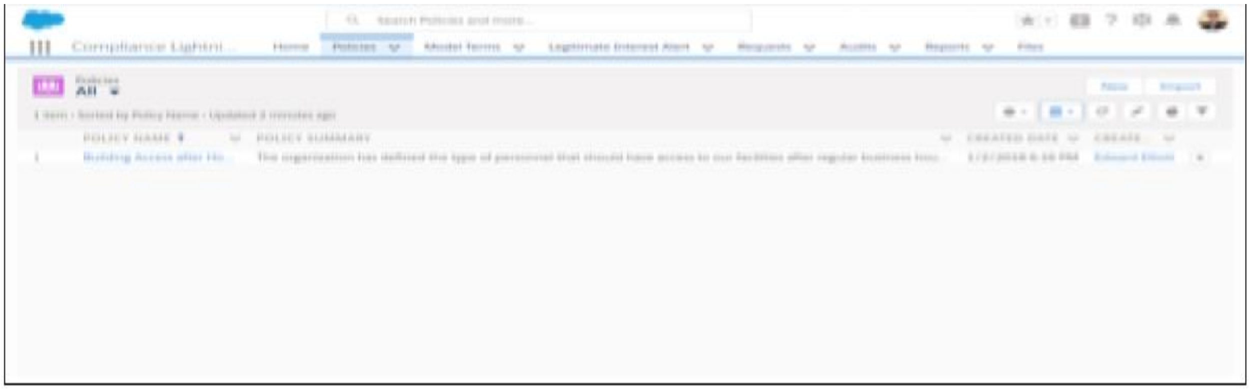
Once you save your policy, it will appear with a flow that defines what status the policy has reached in your review and approval process. You can view the policy in a list-view or a Kanban to manage your review and policy action plan.



1 item • Updated a minute ago

Drafted (1) | Reviewed (0) | Circulated (0) | Approved (0) | Published (0) | Archived (0)

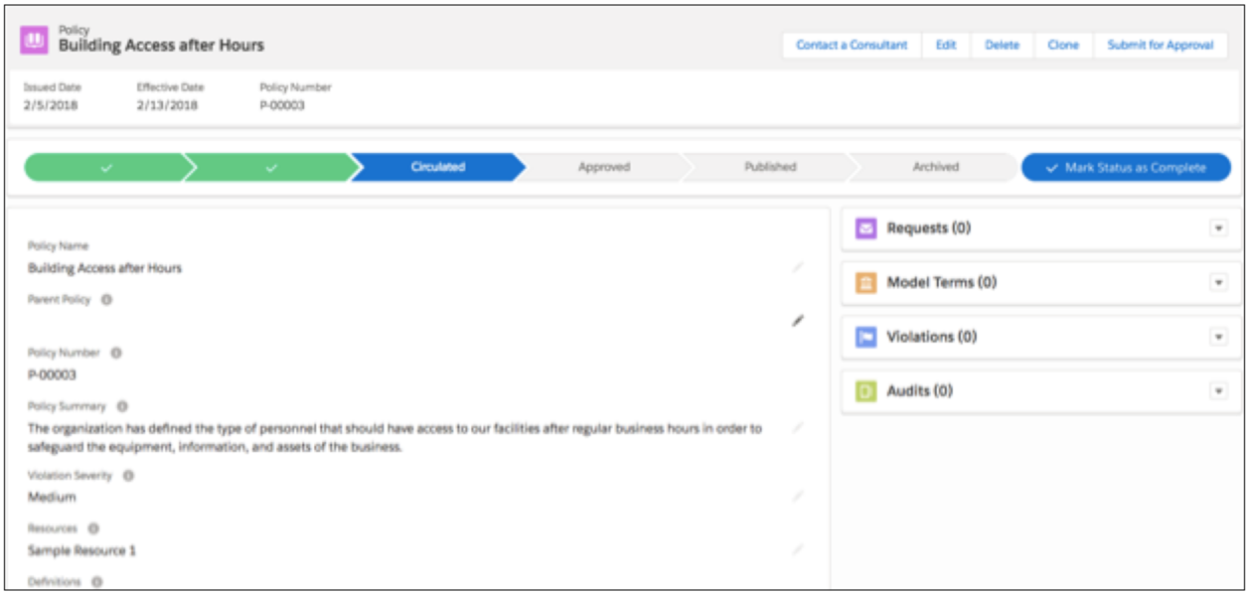
Building Access after H...
The organization has defin...
1/2/2018 6:16 PM
Edward Elliott



1 item • Sorted by Policy Name • Updated 3 minutes ago

	POLICY NAME	POLICY SUMMARY	CREATED DATE	CREATE...
1	Building Access after Ho...	The organization has defined the type of personnel that should have access to our facilities after regular business hou...	1/2/2018 6:16 PM	Edward Elliott

The policy will look like the image below and displays a path to describe the next steps that need to be taken to move the policy forward in your system.



Policy
Building Access after Hours

Issued Date 2/5/2018
Effective Date 2/13/2018
Policy Number P-00003

Policy Name
Building Access after Hours

Parent Policy

Policy Number
P-00003

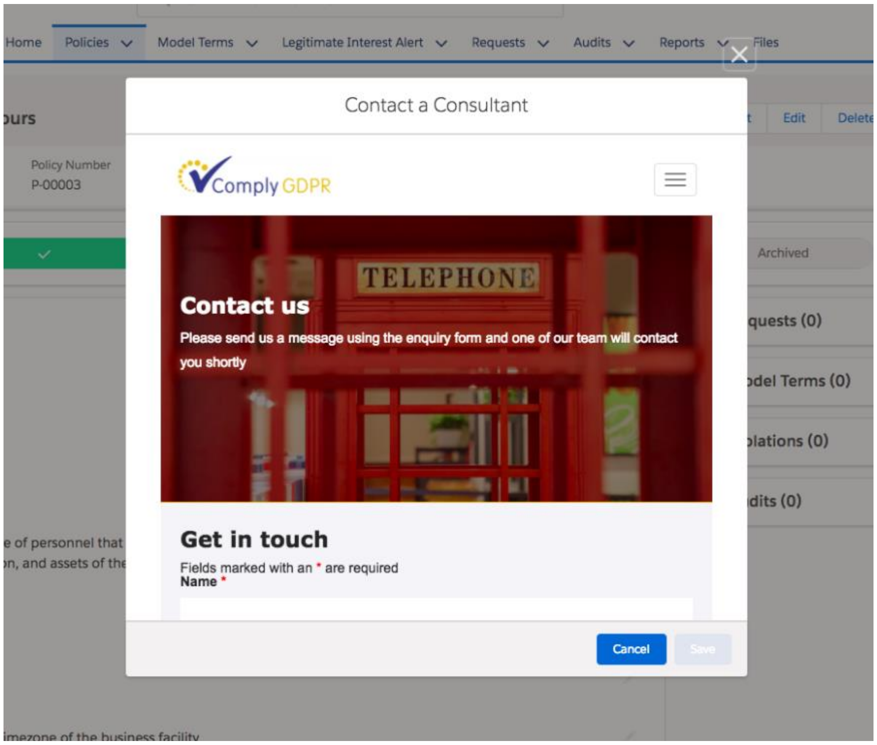
Policy Summary
The organization has defined the type of personnel that should have access to our facilities after regular business hours in order to safeguard the equipment, information, and assets of the business.

Violation Severity
Medium

Resources
Sample Resource 1

Definitions

If you need assistance defining your policies click the **Contact a Consultant** button to reach a policy consultant who can assist your organization in the definition of your GDPR policies.



Contact a Consultant

Contact us

Please send us a message using the enquiry form and one of our team will contact you shortly

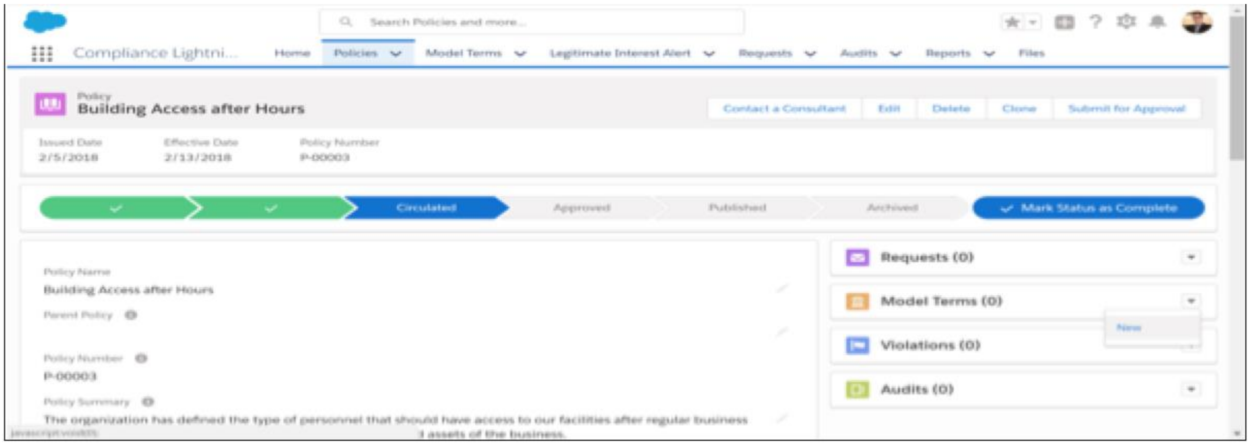
Get in touch

Fields marked with an * are required

Name *

Step 4: Define Model Terms

You can now review which policies require model terms for your website and/or contracts.



Policy
Building Access after Hours

Issued Date 2/5/2018
Effective Date 2/13/2018
Policy Number P-00003

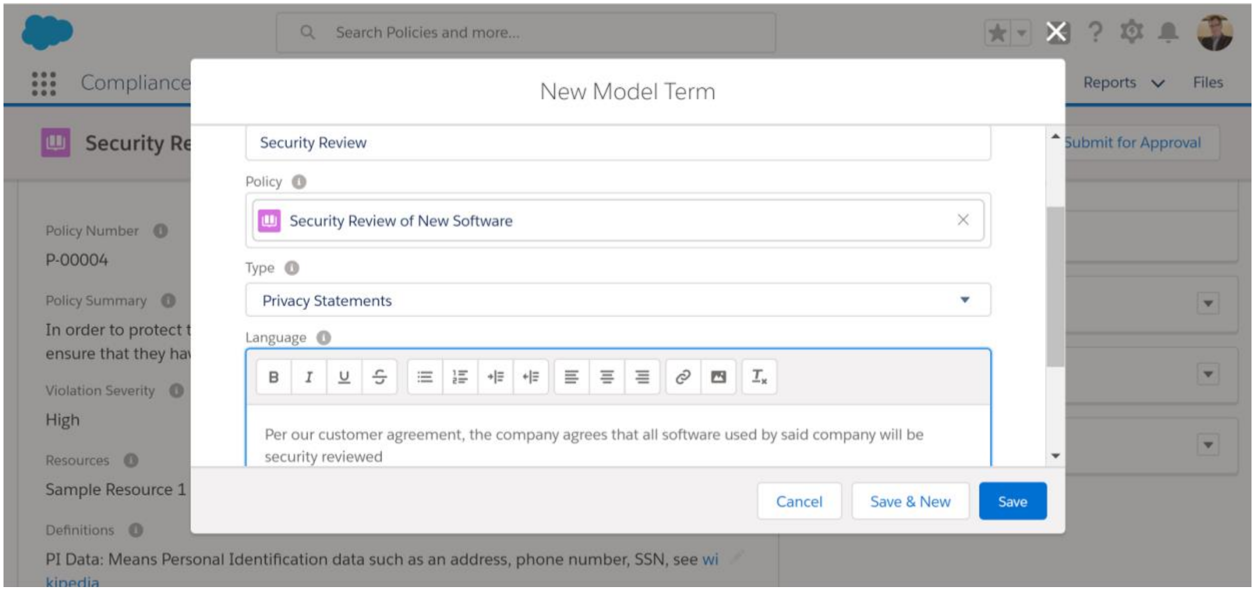
Policy Name
Building Access after Hours

Parent Policy

Policy Number
P-00003

Policy Summary
The organization has defined the type of personnel that should have access to our facilities after regular business
...d assets of the business.

From the policy, you can create a new model term to be used as a standard in the implementation of the policy. The model terms are defined to be used in clauses, documents, privacy statements, agreements, and checklists that are used for distribution to third parties. The model terms will provide a library of acceptable language to be used with external points of contact.



New Model Term

Security Review

Policy
Security Review of New Software

Type
Privacy Statements

Language
Per our customer agreement, the company agrees that all software used by said company will be security reviewed

Security Re...

Policy Number
P-00004

Policy Summary
In order to protect t...
ensure that they ha...

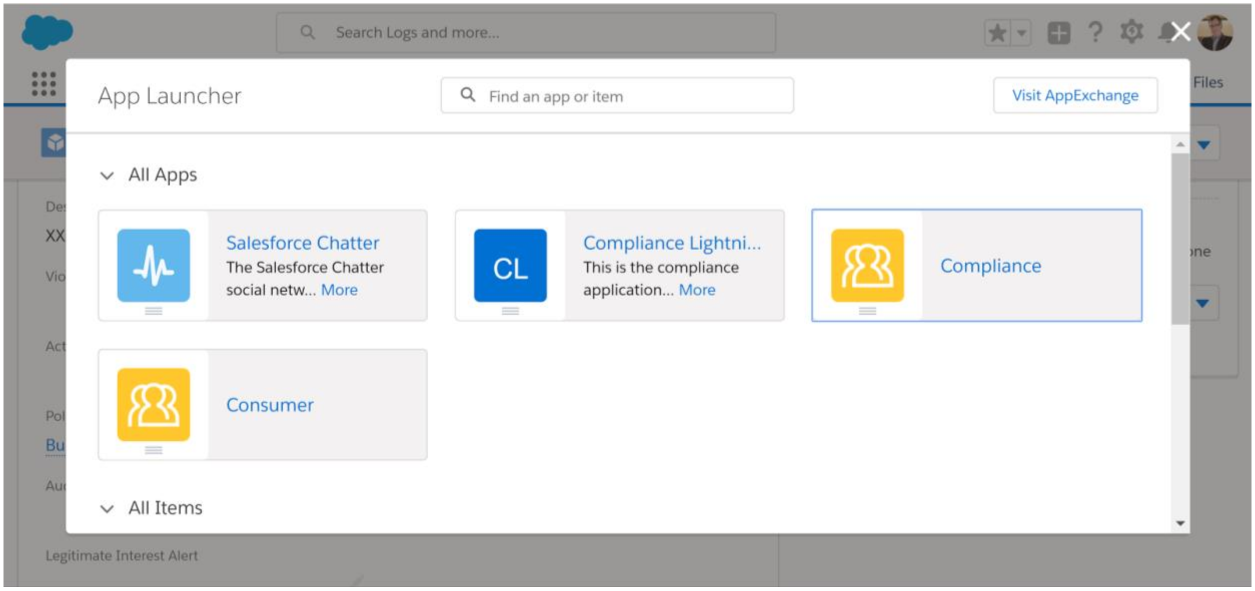
Violation Severity
High

Resources
Sample Resource 1

Definitions
PI Data: Means Personal Identification data such as an address, phone number, SSN, see wikipedia

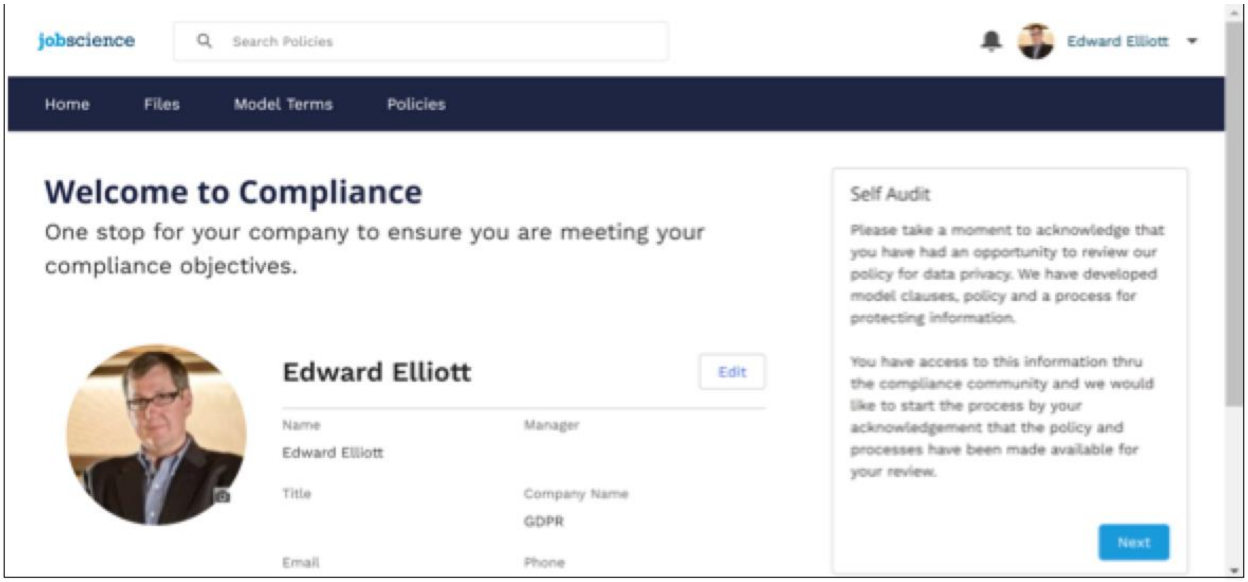
Step 5: Create Your Employee Community

Employees who need to be aware of your policies, but are not active in the management of the policy, should access the information via a defined Employee Community. You should define the audit and review activity with your legal counsel and/or consultants.



The Salesforce Chatter social netw... More

This is the compliance application... More



Welcome to Compliance

One stop for your company to ensure you are meeting your compliance objectives.

Edward Elliott

Name: Edward Elliott

Manager:

Title:

Company Name: GDPR

Email:

Phone:

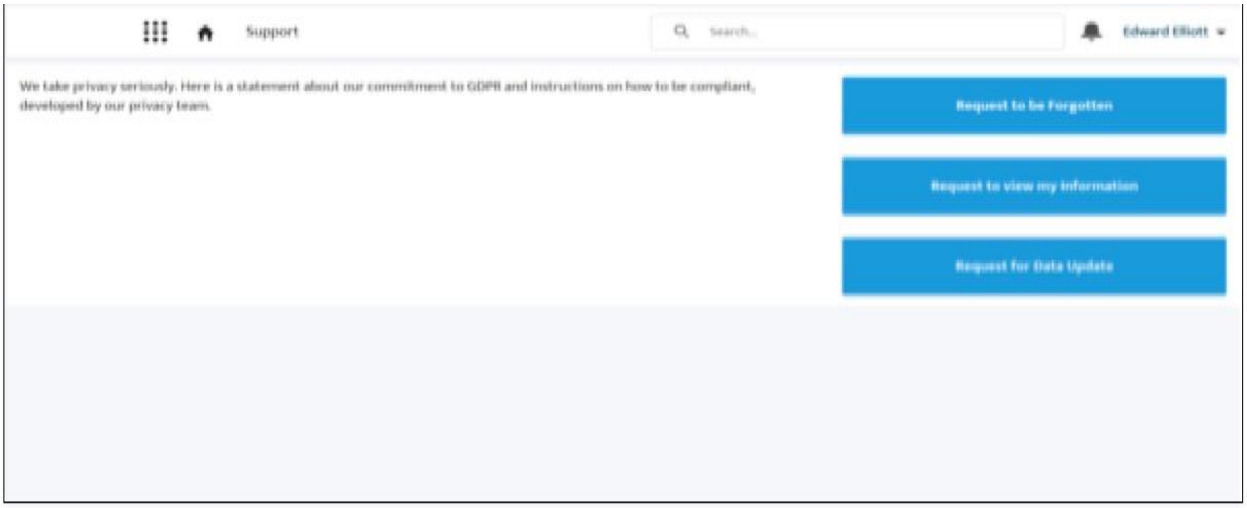
Self Audit

Please take a moment to acknowledge that you have had an opportunity to review our policy for data privacy. We have developed model clauses, policy and a process for protecting information.

You have access to this information thru the compliance community and we would like to start the process by your acknowledgement that the policy and processes have been made available for your review.

Step 6: Create Your Consumer Community

It’s important that you provide third parties with a way to make requests of your organization regarding policy requests. We recommend that you provide simple forms for individuals to make requests appropriate to you policies. You should define the request process and activity with your legal counsel and/or consultants.



We take privacy seriously. Here is a statement about our commitment to GDPR and instructions on how to be compliant, developed by our privacy team.