METAPOLICY

MetaCompliance

MetaPolicy enables organisations to automate and manage the key tasks associated with policy management. From creation and management to publishing and delivery, the cloud-based policy management software enables organisations to measure and demonstrate the continuing improvements in awareness, and highlight areas that require attention before they pose a risk to security and compliance.

Using MetaPolicy, organisations can increase policy participation, conduct risk assessments, easily obtain employee attestation to key policies, and embed a culture of compliance.

METAPOLICY WILL DELIVER:

- The MetaCompliance Policy Management software contains all the key elements required to automate, deliver and manage the policy management life cycle.
- It addresses the key business problems of demonstrating compliance with legislative requirements and proving due care to third party auditors and regulators.
- The software allows organisations to regularly test and risk assess users on their knowledge of corporate information security and compliance practices with minimal time and effort.
- Content can be targeted to specific groups of users based on job role.
- MetaPolicy provides an account of compliance awareness levels, and detailed management reports enable organisations to pinpoint key areas that present risks to data security.

METAPOLICY

MetaCompliance

METAPOLICY BENEFITS

Minimise the Effort and Cost of Policy Management
Obtain employee attestation of staff policies and avoid the need for management to chase staff participation and sign up, saving vast amounts of time.

Automated Policy Lifecycle
Streamline processes and provide a single source of truth for all compliance-related activities.

Obtain Policy Affirmation
Track policy attestation across the organisation and embed a culture of compliance.

Mitigate Risk of Financial Sanction and Reputational Damage
Automate the policy lifecycle and provide the "evidential weight" required to protect organisations from brand degradation and reputational threats.

Increase Staff Knowledge of Threats, Risks and Controls
Regularly assess users on their knowledge of corporate information security and compliance practices with minimal time and effort.

Measures Improvements in Awareness
Measure and demonstrate the continuing improvements in awareness to highlight areas that require attention before they pose a risk to security and compliance.

METAPOLICY FEATURES

Target Unique Groups or Departments

Target or exclude specific groups of users based on job role to ensure that the right policy is going to the right people, at the right time.

METAPOLICY

MetaCompliance

Microsoft Teams App

With the MyCompliance Teams App, users can complete policies without leaving the familiarity of the Microsoft Teams platform. This helps to increase user engagement, improve adoption levels and make attestation easier for end-users.

Microsoft Teams Integration will deliver:

- Enables users to complete their Security Awareness Training and policies without leaving the familiarity of the Microsoft Teams platform.

Attach a Survey to a Policy

Create and attach surveys to policies to help obtain staff affirmation of content and embed a culture of compliance in your organisation. Assigning a pass mark to a survey confirms that the obtained knowledge is correctly applied and stimulates the end-user's knowledge retention.

Automatic Reminder Emails

Send automatic weekly reminder emails to uncompliant end-users to increase user engagement and save admins time.

Deliver Policies to User Desktops

Deliver pop-up messaging on the end-user's desktop for Microsoft Windows based clients.

Robust Reporting Suite on Policy Compliance

Provide a clear audit trail that records who has interacted with policies and help identify the areas that present the highest risk to data security.

Central Repository

Store, manage and distribute policy content on our centralised, cloud-based policy management system.

Version Control

Keep a clear record of how policies were created, developed and changed over time with version control. Ensures that only the latest version of a policy is being used.

PRODUCT ADD-ONS

MetaEngage Add-on

- Content can be targeted to specific groups of users based on job role, and the software's unique ability to obtain employee attestation of staff policies ensures compliance.
- The software contains unique functionality that enables Microsoft Windows based clients to pop up messaging on the user's desktop.
- Client communication functionality is managed from the MyCompliance cloud solution.
- MetaEngage add on provides an account of compliance awareness levels, and detailed management reports enable organisations to pinpoint key areas that present risks to data security.

MetaIncident Add-on

- MetaIncident provides a platform for staff to report any cyber security issues.
- This enables organisations to respond to the reported incidents in a timely manner.
- The incident management functionality with the MetaIncident module provides a lifecycle view of incident management and provides an incident register to manage issues.
- The system provides necessary audits to report to regulators and governance committees.

API

- The Customer API is hosted on Azure App Services and can be accessed via the Azure API Management Application. This provides a method of collecting data from MyCompliance without the need to log on to the platform and perform a manual task.

On-Prem AD Sync

- On-Prem AD Sync enables organisations to sync users directly from an on-premises Active Directory. AD Sync will replicate your organisation's Active Directory on to the platform for targeting purposes. The AD Sync tool updates on a daily basis to reflect joiners/leavers/changers. Users benefit from SSO.

Enhanced Support - Enhanced Support Provision

To supplement the support provided as standard, enhanced support customers will receive the following:

- Enhanced business hours: Monday to Friday (excluding U.K. Bank Holidays) from 08.00 GMT to 22.00 GMT.
- Call logging by email to support@metacompliance.com and by telephone to 00 44 2871 359777.
- A nominated Customer Success Manager who will be an escalation point for the customer should the customer require additional assistance from MetaCompliance.

Deepfake Awareness Training:

- Artificial Intelligence is applied to Customer source material to create engaging eLearning, leading to an increase in end users awareness of how Deepfake technology can be utilised.

SERVICE MANAGEMENT

Service Levels

Severity	Definition	Target Response Time
Priority 1	Critical Problem Serious impact of the Licensee's business operation. The Licensee's ability to progress work is at a standstill or is very seriously impaired. All or most users are affected.	2 Hours
Priority 2	Moderate Problem It is difficult to achieve operational objectives and day-to-day businesses are affected. A substantial number of users or a functional business area is impacted e.g., a department.	4 Hours
Priority 3	Low Level Problem The Licensee can carry out most or all their daily tasks. Could range from a few users moderately affected to all users with a minor problem.	12 Hours
Priority 4	Minor Problem The issue is minor and affects one or two users.	24 Hours
Priority 5	Information Request A user has asked for some information not readily available to first line support.	Best Endeavors

DATA BACKUP AND DISASTER RECOVERY

MetaCompliance operates within a certified ISO 27001 environment, where BCP and DR are core components. Within our cloud platform, we operate an Active Passive plan and use geo-replicated databases, storage and scalable web services. The replicas are in a geographically separate data centre and we utilise DNS traffic directors to manage traffic flows to available points of presence.

ON-BOARDING AND OFF-BOARDING

On-boarding -

1. Provision access to purchased modules
2. Arrange welcome call to begin on-boarding project
3. Agree objectives with customer to be completed as soon as mutually possible during the initial days of your subscription
4. Complete interactive training sessions on all purchased modules and platform
5. Complete any necessary technical requirements in relation to user on-boarding
6. Provide assistance with an initial pilot with a specified group of users
7. Proceed to go live to all required staff with guided assistance
8. Discuss requirements of the platform for the remainder of your subscription
9. Confirm all customer objectives have been achieved and value has been obtained
10. Complete on-boarding and meet with Customer Success Manager

Off-boarding -

1. Customer to export any required reports from the platform
2. Stop all access to platform for admins and users on an agreed date
3. Delete all data and customer platform permanently

SERVICE CONSTRAINTS AND CUSTOMISATION

Metacompliance will apply all commercial and technological efforts to make the software available with a Monthly Uptime Percentage (defined below) of at least 99.99%, in each case during any monthly billing cycle. This monitoring includes monitoring and alerting on all services used on the MyCompliance Platform. The Status of the Platform can be checked at any stage here.

"Monthly Uptime Percentage" is calculated by subtracting from 100% the percentage of minutes during the month in which the Products and Services were unavailable to the Licensee.

SUPPORT AND DOCUMENTATION

MetaCompliance provides support online via documentation and videos. These support resources, known as the Knowledge Base, are accessible once logged on to the MetaCompliance software.

Before any support request is made to MetaCompliance, users shall in the first instance, attempt to resolve their queries and identify the cause of the given problem, using the online support materials available via the Knowledge Base help functionality.

METAPOLICY

MetaCompliance

MetaCompliance's support desk will be manned by competent staff providing Administrative Users with technical support and advice on the use of MetaCompliance software by email in clear written or spoken English.

Administrative Users can contact MetaCompliance's support staff during standard business hours, to raise any concern or queries regarding the use of MetaCompliance software.

Standard business hours: Monday to Friday (excluding U.K. Bank Holidays) from 09.00 GMT to 17.00 GMT.

By email to **support@metacompliance.com**.

All enquiries will be logged in our helpdesk software and issued with a unique ticket reference.

All support enquiries should be responded to within 12 business hours.

COMPENSATION

Should MetaCompliance not meet the service levels agreed at the outset of the service provision, the dispute resolution clause detailed in the G-Cloud 14 contract shall apply. Should such a resolution not be achieved, the buyer has the right to terminate the contract in accordance with agreed terms.

ORDERING AND INVOICING PROCESS

Upon receipt of a completed G-Cloud 14 Call-Off Contract, the MetaCompliance finance department will issue an Acknowledgement of Order. This will be followed by the issuance of an invoice, for the first 12 month period of any G-Cloud 14 contract term, payable within 30 days of receipt. The relevant terms of a mutually agreed G-Cloud 14 contract shall apply.

TERMINATION OF CONTRACT

Written notice must be provided to the relevant contact, as provided in the G-Cloud 14 Call-Off Contract agreed between the parties. Such notice shall be in accordance with G-Cloud 14 Call-Off Contract clause 18 'Ending the Call-Off Contract'.

AFTER SALES SUPPORT

MetaCompliance installs and maintains all services and components that are purchased for the duration of the contract.

METAPRIVACY

MetaCompliance

TECHNICAL REQUIREMENTS

Please ensure that all users are on the latest version of the supported browsers to guarantee the full performance of MetaPrivacy:

- Google Chrome
- Safari
- Microsoft Edge
- Firefox

ALLOW LIST REQUIREMENTS

For all customers:

To successfully receive the emails from the MyCompliance Platform, we will provide you with IP Addresses to 'allow list' within your organisations' security infrastructure (e.g. firewalls). These will be provided for security reasons, once onboarding commences.