Security Policy

Current Offerings

28 June 2023

Contents

1 Description

If you take this policy, we will help you to define and implement a security policy that meets the needs of your business. This means we will:

a) Identify and document with you the physical and information assets in your business and the systems that you use to run your business, including third party cloud systems.

b) We will guide you through the process of analyzing the risks to your business, creating a risk register and then develop strategies for mitigation and contingency. Note: this will focus on the physical risks to your systems and the security risks associated with your people and systems, rather than business or commercial risks related to, for example, competition or market conditions.

c) We will advise you of example statutory requirements, industry specific regulatory requirements where we are aware of the application to your particular business and industry standard frameworks for meeting any obligations.

d) We will then work with you to create a document that describes a security policy that is appropriate to your business.

e) Where any of the above documents already exist in your business, we will instead review those and suggest enhancements or changes to provide effective defences against the current security threats.

f) We will then define the processes that you should follow, either as regular activities to maintain your defences or as activities to undertake if a particular event occurs.

g) Optionally: we can load this security policy and its associated workflows into our cloud cyber security policy monitor workflow engine so that you can monitor the security events impacting your business and take consistent and agreed actions to remediate them when its necessary to do so.

If you take our Remote Monitoring Service, our Business Continuity Service or our Vulnerability Scanning service then data generated by those services will be ingested into the Policy Monitor engine so that your corporate information is maintained up to date.

We can investigate developing interfaces to other equivalent products if you have already got those deployed.

2 Commercial Terms

2.1 Initial charges

There is an initial charge for professional services to document your existing environment, carry out a risk review, develop a security policy to ensure that your environment is protected, define the workflows and present this to your board or operations team for sign off.

2.2 CSPM platform

If you require us to implement it then we will load the policy and workflows onto the Cyber Security Policy Monitor platform then assign individual staff or roles to each of

the tasks. The cost of this will be $1 / user / month for all users in the business who operate IT systems and therefore contribute in some way to the security of the business.

You will pay a single monthly subscription in advance for the ongoing Policy Monitor service.

If you already have alternative technology deployed that is equivalent to our Remote Management service, our Business Continuity Service or our Vulnerability Assessment service then there will be a small recuring charge to for us configuring and operating the interface to those products.

When you take our service there is an initial 1-year commitment. You can terminate use of the service completely giving 30 days' notice on completion of the 1-year commitment.

If you terminate the service, then your users will no longer be able to login.

Your charge is monthly in advance for payment within 15 days. We can take check or credit card but request you set up regular ACH payments to minimize administration and costs for both parties.

A small discount is available for increased long-term commitment or annual payments in advance provided payments are via ACH.

3 Service benefits

The benefits of this service are that:

a) The board can demonstrate that they take security seriously, that they review security on a regular basis at board level and that they have put in place the policies to provide a robust defence to cyber-attacks.

b) The board can monitor in real time compliance of staff across the company with the security policy and can act on if there is no evidence of policies being followed.

c) If other Services are taken, then the data outputs from these services can be ingested automatically identifying a problem and potentially triggering radiation activity directly.

d) In the event of a security breach occurring, the organization had evidence that they have defined an effective policy, they have put it into action, they have responded to an event appropriately and in accordance with practiced approaches.

e) The cost of creating or reviewing a policy is minimized because we can base a proposed policy on industry standard activities which the organization can review and accept, modify or reject depending on the needs of the organization, minimizing the effort to create a policy from scratch.

f) However, that policy can easily be modified in the future as the organization reviews the threats, the associated risks and the number of incidents that have occurred so that a cost-effective approach is always followed that can respond to a changing threat level.

4 Deploying and Operating the Service

If the organization wishes to manage the security policy using their own existing systems, then there is no operational system to deploy and operate.

If the organization wishes to use our Cyber Security Policy Monitor workflow engine to manage the policy, then the steps are as follows:

a) A profile for the organization is created in our cloud-based solution.

b) Users are added to the system, either individually or by uploading a csv file containing names, email addresses and primary system roles.

c) An administrator then assigns users to roles which controls the tasks that each user may be required to carry out.

d) The security policy is reviewed and the frequency it is expected that regular tasks will be undertaken, or the expected frequency of external events occurring is adjusted.

e) Regular tasks are then activated, and users prompted to carry them out when they are due.

f) Any appropriate systems within the organization which are supported by our solution are connected and then generate events in the system when activity is required.

g) The executive team can then monitor and report on the organization's compliance with the security policy.

This service is generally available 24 x 7 x 365 but we may shutdown the system temporarily to perform software upgrades and other routine maintenance, in which case we will provide you a minimum of 48hrs notice. Any such shutdowns should be outside the working day in the geography where you are based.

5 Supporting Documentation

An electronic copy of the security policy is maintained and provided to the customer for review on a regular basis.

The risk register is maintained online and can be inspected whenever required.

Definitions of the workflows can be reviewed online and adjusted from time to time as required.

There is a user guide for the system, provided as a consolidated document but also available as individual pages attached to the relevant screens the use of which they are describing.

There are additional videos and other collateral describing the tasks that make up workflows.

An auditor who wished to inspect activity and progress over time can review on a calendar basis compliance with the security policy.

6 How Support Works

The following is a brief description of our support mechanism. This is explained fully in our support manual:

- If you have an issue with our solution, then you can raise it via our service desk which is accessible from the help button or use the report an issue

screen to report directly from the solution. Once it arrives with us, we then triage that problem.

- We may merge incidents reported for many devices if they are fundamentally the same problem, and particularly if you took another of our services that would report problems with the network.
- All information related to the issue should be entered via service desk, but we will accept calls to escalate urgent/serious issues by email or phone.
- Once an issue is raised, you can then track the issue through to resolution.
- All our solutions use the same support desk instance so it's possible that related issues from our other series may be merged into a single issue.

Support is provided during the working day between 0800 and 1800. Optionally you can purchase extended support for out of hours or 24 x 7. We may not be able to implement 24 x 7 support immediately and need a notice period to put in place.

At the end of each month, you are provided with a report describing our performance against agreed KPIs.

Our service desk is available at the following URL

https://cysure.atlassian.net/servicedesk/customer/portal/2

7 What is not included

Once the initial period of consultancy is completed this service reverts to an online service only, with support provided through our support desk facility.

Onsite support is not included as part of this service: However, we would be pleased to provide additional on-site services or specific consultancy by you taking additional days of effort through our Assistance Consultancy services.

You can take this service as your only service from us. The full benefit of using the Cyber Security Policy Monitor service is only likely to be obtained if you also take the Remote Management service and Business Continuity service or have similar technologies already in place with an alternative vendor with whom we can communicate.

8 How we may change the service from time to time

We will upgrade Cyber Security Policy Monitor from time to time and we will publish details of planned outages in advance.

We may increase the number of interfaces we support to external technologies from time to time.

We will update the templates in the system from time to time on which we based security policies. This should not normally affect your current security policy.

We will change the user interface from time to time. When we do so we will re-issue our support material such as help text or videos.

Our service is based on purchasing software subscriptions from our cloud supplier which we then use to deliver the service. From time to time the technology vendors of these products increase their prices and we need to similarly increase our prices.

We will publish any revised prices on our website and will notify you of any price rises giving you 3 months' notice of such price rises. By taking this service you agree to accept any such price rises. You may terminate the service if you wish.

We may change the URL by which you access the system, in which case we will re-direct the previous URL to the replacement URL for a period which we will advise to give you time to change any documentation or browser bookmarks that you may hold.

9 Terminating our service

When you subscribe to the service you commit to an initial period of one year. On completion of this initial term, you can terminate the service at any time giving us 30 days' notice.

On termination and provided we have received payment in full on all outstanding invoices, we will on request provide to you an export of all your data in the system in CSV form. Our data model is confidential, and you are not permitted to reverse engineer this from our data export.

After one month or sooner if you request, we will export all your data then details of the devices from our management platform and then remove all details of your organization from the platform. We will delete that export if you request or after a year whichever is the sooner.

If you wish to restart use of the service within one year, we can reload your data from out export.

It is your responsibility to archive any reports important to you before you terminate because once we remove your organization from the platform all historic data is deleted.

If you require any assistance from us when terminating, for example to understand the export format and then to reload your data into an alternative solution, then as a responsible supplier we will assist you in this process if requested and charge you at our standard professional services rates on a time and materials basis.