Securepoint GmbH
Bleckeder Landstrasse 28 21,337 Lüneburg
Tel.: +49 4131 / 24 010
www.securepoint.de | info@securepoint.de

Securepoint Awareness PLUS
- Description of Services -

Date: 01 December 2021 – Version: 1.0 – Author: Eric Kaiser

Service Elements

Securepoint Awareness PLUS consists of two building blocks (hereinafter “Service Building Blocks”). These are Phishing simulations and the provision of e-learning modules based on these simulations. The Service Building Blocks are partially web-based.

Prices

All prices are to be found in the current pricelist.

The total number of Users for all licenses assigned to a partner/reseller is determined monthly on a reference date determined by Securepoint and billed based on the prices in the current pricelist.

A User is any active user with an account on the Awareness Platform (manager.awareness.securepoint.cloud).

Term of Contract

The reseller generates a separate license for each customer. The license has a minimum period of 12 months from creation of the first user account within that license. The contract shall automatically be renewed by a further 12 months when notice of termination is not given at least 4 weeks before the end of the term.

Billing

The billing period is one month. Billing takes place monthly on a retroactive basis. Incomplete months shall be charged as full months. Billing is based on a monthly reference date to be determined by Securepoint. As a rule, that date remains the same every month.

Product Offering Enhancement

Securepoint reserves the right to extend, supplement or amend individual services at any time insofar as this results in an improvement to service for customers or does not encompass any (significant) adverse effect for customers.

General

Securepoint provides its platform including the services to be delivered via that platform on servers to be used at the access point of the data centre of Securepoint or its partners (“service handover point”). In order to use the platform, customers must have their own internet access which allows them to access the platform at the service handover point.

Customers and users must keep login details, passwords etc. for accounts and user accounts secret and not pass them on to unauthorised third parties (or other users). They must actively log out after any login session. This also applies to login data for a Single-Sign-On system, with the exception that manual logging out is not mandatory after every access of the system. Declarations and actions undertaken via an account/user account after login with the password and email address of a customer or user may be attributed to the customer, regardless of whether the customer is aware of them. Attribution takes place in particular when the customer or a user deliberately or negligently allows a third party (including a family member) access to a password or account/user account. In the case of a well-founded suspicion that access data may have become known to an unauthorised third party, Securepoint is entitled but not obliged, for security reasons and at its own discretion, to change a customer or user's login details (without prior warning) and/or to temporarily block the account/user account. Securepoint shall inform the customer or user of this action without delay and issue new login details within a reasonable timeframe. The customer and/or user has no right to demand that the original login data are restored. In the case of Single-Sign-On, only access via this Single-Sign-On with existing access details will be blocked, and the customer or user can only log in with the new login details. The new login details may once again be integrated in a Single-Sign-On.

Simultaneous use of the same account via multiple end-user devices is not permitted.

Except where expressly permitted by Securepoint, registration of users with private email addresses is not permitted; this applies in particular to free email services such as GMX, Web.de or Google Mail.

Rights of Use and Copyright

Securepoint assigns to the customer the geographically unrestricted, temporary, revokable, non-exclusive, non-assignable and non-transferable right to use the platform and the Service Building Blocks made available thereupon, along with additional services, for the customer's own operational purposes, for the number of users and in the scope specified in the Awareness-Building contract.

The customer is not authorised: (i) to rent, lease, loan, reproduce, resell or in any other way market or share the platform or access to the platform, including via the internet or upstream/downstream public or private network; (ii) to use the platform to develop other services; (iii) to activate or use elements of the platform for which the customer has not been granted usage rights; (iv) to assign usage rights for the platform to a third party or to grant a third party access to the platform; (v) to change, translate, reproduce or decompile the source code of the platform, or to investigate its functions, except where this must be permitted by law pursuant to Articles 69d and 69e of the Act on Copyright and Related Rights ("UrhG"); (vi) to remove, obscure or change legal notices, in particular relating to the commercial property rights of Securepoint.

Insofar as Securepoint enables a customer to create own materials using the platform (evaluation of e-learning, evaluation of phishing simulations, etc.) or provides such materials, individually tailored to the customer, for download and printing, Securepoint assigns the customer, upon full payment of the agreed fee, the indefinite, geographically unrestricted, revokable, non-exclusive, non-assignable and non-transferable usage rights to all material prepared by Securepoint for the customer within the scope of this contract, to the extent that such assignment is possible according to German law and in the actual situation.

Securepoint reserves the right to make use of the above-mentioned individual materials (excepting all external brands and trademarks) and, in particular, the findings thereby acquired, for its own purposes.

Guarantee

Regarding usage of the platform, the Service Building Blocks provided via the platform and additional services, defects are covered by the provisions of Articles 536ff of the German Civil Code ("BGB") and points 3.2 to 3.5 below:

Liability without fault shall not be accepted for initial defects pursuant to Article 536a Paragraph 1, 1st variant of the German Civil Code ("BGB"). Securepoints fault-based liability remains unaffected.

Defects shall be resolved either by reworking or replacement, free of charge, at Securepoint's discretion.

The customer shall only be entitled to terminate the contract due to the failure to enable contractual use, pursuant to Article 543 Paragraph 2, Subparagraph 1 No. 1 of the German Civil Code ("BGB"), when Securepoint has had sufficient opportunity to resolve the defect and has failed to do so.

Securepoint assumes no guarantee for the customer's internet access, in particular for the availability and scale of internet access. The customer assumes responsibility for its own internet access up to the service handover point.

Service Level Agreement (SLA)

Applicability

The Service Level Agreement details and specifies the quality and scope of services offered by Securepoint GmbH (hereinafter "Securepoint"). A contract is agreed between Securepoint and the customer for the provision of services in the field of employee training and awareness building (hereinafter "Main Contract"). The service provider, Securepoint, and the service recipient (hereinafter "Customer") are hereinafter jointly referred to as the "Parties".

This document contains all relevant provisions and rules to detail the service description for awareness-building services and duty to cooperate in the Main Contract bewteen the Parties.

Prerequisites and Duty to Cooperate for the Usage of the Services

General Prerequisites and Duty to Cooperate

Various elements of the following Service Building Blocks (Point 3) require access to web pages of Securepoint using a web browser. Only the following browsers are supported for this purpose, and usage of one of these browsers is a prerequisite for the provision of service:

Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge and Microsoft Internet Explorer 11, in each case in the current version.

Special Prerequisites and Duty to Cooperate

The special prerequisites and duty to cooperate for the usage of awareness-building services are listed in Point 3 for the individual Service Building Blocks.

Service Building Blocks

The following sections describe the services offered by Securepoint and determine the processes and organisational interfaces necessary for service provision.

Phishing Simulation

The Phishing Simulation Service Building Block encompasses the sending of a defined number of emails (emails to be agreed in advance) to users over the service period. These emails simulate genuine phishing emails and are intended to raise user awareness of the IT security risks posed by phishing attacks. Clicking on a phishing element (e.g. image, link) in a simulated phishing email opens a web page (hereinafter “Learning Page”) which instructs the user about the simulation and provides specific advice on how the email could have been identified as a phishing attempt.

To ensure the delivery of all simulated phishing emails to all users to be trained in the context of the training, the Customer needs to establish a whitelist. This is a duty to cooperate for the Customer, without which Securepoint can not ensure provision of the contractual service. In this matter, the Customer thus bares responsibility for the simulated phishing emails being delivered in their entirety to user mailboxes so that they may be used within the framework of the training measure. Should the Customer not be able to influence whitelisting directly (e.g. because the Customer has entrusted an IT service provider to administer its IT systems), the Customer is nevertheless responsible to ensure that the whitelisting takes place.

The following steps must be undertaken for whitelisting:

Securepoint’s dedicated email server must be added to a whitelist for the receiving mail system in order to prevent inbound emails from being rejected.

Any filter systems on the customer side (e.g. secure email gateways) must be configured in such a way that the simulated phishing emails are not marked as “junk” or “spam” and delivery to the users can be guaranteed.

Any systems on the customer side to protect internet access from end-user devices (e.g. web gateways, proxies, operating system security settings) are to be configured in such a way as to ensure the unfiltered display of simulated phishing emails in the users’ email clients. Furthermore, these systems are also to be configured to show the Learning Pages in a web browser.

Securepoint provides a guide for the implementation of these steps. The guide contains all the necessary technical information such as IP addresses and server names for the email server along with URLs to be permitted by filter systems and access protection systems.

Access via Learning Platform

Securepoint’s proprietary learning platform is reachable at https://awareness.securepoint.cloud. Users may register here with their work email addresses. Alternatively, anonymous access codes may be used.

Securepoint Manager

Customers can access the Securepoint Manager online at https://manager.awareness.securepoint.cloud. The Securepoint Manager is the portal for administration of awareness measures. Within the reporting dashboard on the portal, the customer can view various key indicators about the service elements ordered, e.g. general click-through rates for simulated phishing emails, overall progress in e-learning or, depending on the service level, the individual e-learning results of individual personnel. Exactly what data can be viewed and edited is covered by a separate AV contract.

Scope of Individual Awareness Packets

The packet can be ordered for customers with 1 to 250 users.

On the self-service platform, https://wiki.securepoint.de, the customer has access to comprehensive instructions that clearly explain to users all necessary steps, e.g. setting up whitelistings.

All relevant information (customer data, billing data, etc.) must be entered via the customer using the platform.

A template Excel file is provided for entering the user list; it is important that the schema of the template is maintained to ensure a clean upload of data to the self-service platform. The customer may update the user list.

Interactive learning modules and videos in the e-learning are fixed and cannot be changed. A suitable industry packet may be chosen for the phishing simulation.

A template Excel file is provided for entering the user list for the phishing simulation and/or the e-learning; the schema of the template must be maintained. The user list is transferred to Securepoint using a secure data connection on the Securepoint Manager Portal. The customer shall receive a user account for this purpose.

The customer may update the user list using this same access to the Securepoint Manager Portal at any time where fluctuation, etc. necessitates change.

A guide to setting up the whitelisting is provided by Securepoint.

For the e-learning, the agreed number or selection of available interactive modules and videos on the subject of IT security may be activated for all of the customer’s users.

The available languages are German and English.

For the phishing simulation

We send 12 simulated phishing emails, randomised, over the course of the year, based on attacks that have been observed, e.g. in your industry. The collection is continuously being updated.

The available languages are German and English.

The evaluation incorporates benchmarks on all key indicators, compared with a customer average.

Users receive a certificate for all modules successfully completed on the Securepoint learning platform.

Gamification: Users on the Securepoint learning platform progress through levels, collect badges and can view their progress in a personalised overview of achievement. (can be activated/de-activated)

Service Availability

General Availability

For awareness building services provided by Securepoint via https://awarenss.securepoint.cloud, the learning pages or the stremaing server, the following minimum average availability (based on the monthly mean) must be met. These requirements are considered satisfied as long as the actual monthly mean availability is not lower than these levels.

Availability is measured as the ratio of uptime (i.e. the time for which the service is correctly available) to total time (uptime plus downtime):

Availability = Uptime / (Uptime plus Downtime)

Availability in percent - converted to minutes for a system that is available 24 hours a day, 365 days per year (24 x 365 = 8760 hours).

E-learning platform: 97%

Securepoint streaming server (access via external LMS): 97%

Learning pages for simulation: 97%

Exceptions to Availability

Maintenance work on the systems of Securepoint and their suppliers, necessary to maintain and secure ongoing operations or for updates and upgrades, do not count as downtime in the sense of the above.

As a rule, maintenance is carried out on weekends between Saturday 09:00am and Sunday 06:00pm or nights on weekdays between 11:00pm and 07:00am the next morning. In exceptional cases, a system maintenance may be carried out at other times, taking into account the smallest possible impact on ongoing operations. In such cases, Securepoint shall inform the Customer of scheduled system maintenance as early as possible, but at the latest one calendar week before the system maintenance.

Shortfall in Availability

For every shortfall in the monthly general availability by one full percent point, except where covered by the “Exceptions to Availability”, the Customer shall receive one additional day of the contractual services at the end of the contractual term.