EMAIL - MANAGED PLATFORM AND CONTROLS SERVICE

SERVICE DESCRIPTION SD201

DOCUMENT CONTROL

Version	Completed by	Date
1.0	Theo Jarvis	13 November 2024
1.1	Theo Jarvis	30 July 2025

PREPARED BY

Name	Job title
Theo Jarvis	Service Development Programme Manager

CONTENTS

1. SERVICE OVERVIEW 5

1.1 SERVICE SUMMARY 5

1.2 SERVICE FEATURE TABLE 7

2. SERVICE DETAIL 9

2.1 SOFTCAT SUPPORT 9

2.2 PLATFORM 9

2.3 ANTI-PHISHING AND MALWARE PROTECTION 10

2.4 QUARANTINE MANAGEMENT AND REMEDIATION 11

2.5 PHISHING REPORTS AND REMEDIATION 11

2.6 POLICY MANAGEMENT 11

2.7 CHANGE MANAGEMENT 11

2.8 REPORTING 12

2.9 SERVICE DELIVERY ASSOCIATE 12

2.10 SIEM INTEGRATION (OPTIONAL ADD-ON) 13

2.11 EXTENDED ARCHIVING (OPTIONAL ADD-ON) 13

2.12 SECURITY INCIDENT RESPONSE (OPTIONAL ADD-ON) 13

3. SERVICE LEVELS 15

3.1 SOFTCAT SUPPORT 15

3.2 CHANGE MANAGEMENT 16

4. CUSTOMER RESPONSIBILITIES 18

4.1 SOFTCAT SUPPORT 18

4.2 PLATFORM 18

4.3 ANTI-PHISHING and MALWARE PROTECTION 18

4.4 QUARANTINE MANAGEMENT AND REMEDIATION 19

4.5 CHANGE MANAGEMENT 19

4.6 REPORTING 19

4.7 SERVICE DELIVERY ASSOCIATE 19

4.8 EXTENDED ARCHIVING (OPTIONAL ADD-ON) 19

5. NOTABLE EXCLUSIONS 20

5.1 SOFTCAT SUPPORT 20

5.2 SERVICE DELIVERY ASSOCIATE 20
6. SERVICE ACCEPTANCE AND ONBOARDING 21
7. SERVICE BILLING AND CONTRACT TERM 22
8. TERMS AND CONDITIONS 23
8.1 OVERVIEW OF TERMS AND CONDITIONS 23
8.2 DATA PROCESSING AGREEMENT AND ACCEPTANCE OF THE CONTRACT 23
8.3 ADDITIONAL TERMS 23
8.4 ISO STANDARDS 24

1. SERVICE OVERVIEW

All bold and capitalised Terms throughout this Service Description are described in the Glossary and definition of Terms.

1.1 SERVICE SUMMARY

Softcat's Managed Platform and Controls Service offers comprehensive email protection against phishing, malware, and sophisticated email threats through advanced threat intelligence and machine learning algorithms. This is delivered from our UK-based 24x7x365 Operations Centre.

The Service comprises:

- 24x7x365 access to log support Cases **("Softcat Support")**
- Access, Onboarding, and Continuous Support of the Platform **("Platform")**
- Inline API-based protection for inbound, outbound and internal email communication **("Anti-Phishing and Malware Protection")**
- Handling and resolution of End-User quarantine release requests **("Quarantine Management and Remediation")**
- Handling and resolution of end-user phishing reports **("Phishing Reports and Remediation")**
- Regularly review and update security policies in line with evolving threats/customer requirements **("Policy Management")**
- Standardised methods, processes and procedures which are used for all changes **("Change Management")**
- Automated reporting delivered via email **("Reporting")**
- A point of contact and escalation **("Service Delivery Associate")**

Optional Add-Ons are chargeable extras and, where required, will be quoted, and confirmed on the Work Order:

- The integration with compatible Security Information and Event Management (SIEM) platforms **("SIEM Integration") (Optional Add-On)**
- Incident response where malicious activity is suspected **("Security Incident Response") (Optional Add-On)**
- The archiving of emails, incoming and outgoing for up to ten (10) years **("Extended Archiving") (Optional Add-On)**
- Providing a named Service Delivery Manager, service reviews and service reporting. **("Service Delivery Manager" (Optional Add-On)**

Together, the above comprise the **"Managed Platform and Controls Service"**, referred to as the **"Service"** within this document.

Security Incident Response is provided in partnership with Check Point and managed by Softcat using the Major Case Management process.

The Service is delivered in accordance with the following ISO standards:

- ISO 20000
- ISO 27001
- ISO 9001

- ISO 22301

Unless otherwise stated in the Work Order, and in addition to any Terms set out in this Service Description, the following applies to the delivery of the Service set out in this Service Description:

- Softcat Terms and Conditions: T&Cs
- The Data Processing Agreement: DPA
- Check Point Incident Response: SLA refer to Section 8.3

1.2 SERVICE FEATURE TABLE

Email – Managed Platform and Controls Service	
Softcat Support	
Log Support Cases 24x7x365 [1]	✓
Online Support portal to track and log calls	✓
A minimum of two (2) authorised contacts	✓
P1 Response Service Level target	✓
Platform	
Onboarding of SaaS application	✓
Infinity portal access	✓
Email security portal for End-Users	✓
Anti-Phishing and Malware Protection	
API-based protection for inbound, outbound and internal email communication	✓
Quarantine Management and Remediation	
Handling and resolution of End-User quarantine release requests	✓
Daily end-user quarantine reports	✓
Phishing Reports and Remediation	
Handling and resolution of end-user phishing reports	✓
Policy Management	
Regularly review and update security policies in line with evolving threats/Customer requirements	✓
Change Management	
Standard Change Requests	✓
Normal Change Requests	✓
Retrospective Change Requests	✓
Emergency Change Requests	✓
Customer performed maintenance	✓
Reporting	
Automated reporting	✓
Customised schedule, weekly or monthly	✓
Service Delivery Associate	
Contact and escalation	✓

SIEM Integration (Optional Add-On) [2]	
The integration with compatible Security Information and Event Management (SIEM) platforms	✓
Extended Archiving (Optional Add-On) [2]	
The archiving of emails, incoming, outgoing, internal for up to ten (10) years	✓
Security Incident Response (Optional Add-On) [2]	
Security Incident Response	✓
Purchase of additional Security Incident Response hours	✓
Flexible use of Security Incident Response hours	✓

[1] Requests are acted upon within contracted coverage hours, as confirmed in the Work Order.

[2] "Optional" and "Optional Add-On" means a chargeable extra. Where a chargeable extra is chosen by a Customer, this is confirmed on the Work Order.

2. SERVICE DETAIL

2.1 SOFTCAT SUPPORT

Authorised Customer Contacts have access to Softcat Support around the clock and on any day of the year ("24x7x365") [1].

Customer Contacts should raise a Case primarily via the Support portal, where the Case type will be assessed, defined and communicated and the priority level will be agreed with the Customer. Where Service Levels apply to the management of a Case, these will be confirmed on the Work Order. For any Case which the Customer believes to be urgent, the Customer Contact must report to Softcat by telephone.

[1] Requests are acted upon within contracted coverage hours, as confirmed in the Work Order.

2.2 PLATFORM

Softcat will work with the Customer to onboard their chosen application into the Platform for Harmony Email and Collaboration, the available supported applications are listed below. As part of the onboarding activity the Customer will be granted access to two (2) portals.

- **Check Point Infinity Portal** – Provides customers a unified security management platform that seamlessly integrates advanced threat prevention across networks, cloud environments, and endpoints. This portal enables centralised visibility of their Check Point estate, management, and automation, allowing Customers to effectively mitigate security risks. For the Harmony Email and Collaboration module, the Customer will only be granted read only access as part of the Service.
- **Email security portal for End-Users** – This portal will be accessible to all users with an active email inbox that have been onboarded into the platform. This portal enables End-Users to view all quarantined emails they have, where necessary request a quarantine release, view the status of a quarantine release and any necessary updates.

Supported SaaS applications:

- Office 365 Mail
- Gmail

Other supported applications may be available upon request, it's recommended that the Customer discuss any additional requirements with their aligned specialist, this may be subject to additional charge which will be quoted separately and detailed in the Work Order.

2.2.1 RETENTION PERIODS

By default, Harmony Email and Collaboration retains emails as follows:

Verdict and enforcement	Raw email (Original email with attachments)	Email meta data (Attributes and data detected from the security scan)
Clean emails (Includes emails with re-written links in the email body)	14 days	14 days
Emails with modified attachments and emails that have cleaned (sanitized) attachments, removed as password-protected attachments, and re-written links	14 days	180 days
Emails containing threats but not quarantined (includes emails with phishing / spam / malware / DLP detection that are not quarantined)	14 days	180 days
Quarantined emails (includes manually quarantined emails)	180 days	180 days
Emails quarantined by Microsoft	180 days	180 days

2.3 ANTI-PHISHING AND MALWARE PROTECTION

Harmony Email and Collaboration platform utilises an API-based integration that allows scanning of inbound, outbound and internal communication in real-time to prevent lateral and insider attacks within the organisation and data leakage. Harmony Email and Collaboration trains Artificial Intelligence on the sophisticated and evasive attacks leading to an overall reduction in phishing emails reaching the inbox.

Harmony Email and Collaboration uses Check Point's SandBlast technology and includes:

- **Threat emulation** evasion-resistant CPU-level sandbox that blocks first-time seen malware.
- **Proactive Threat Extraction** cleans files and eliminates potential threats to promptly deliver a safe file version to users.
- **Threat Extraction** maintains uninterrupted business flow, while the sandbox continues in the background. Threat Extraction eliminates unacceptable delays created by traditional threat emulation, while instantly cleaning files of any active content.

To prevent outgoing emails from failing SPF ("Sender Policy Framework") checks and being quarantined, the Customer is required to add the following to their SPF records: **include:spfa.cpmails.com**

2.4 QUARANTINE MANAGEMENT AND REMEDIATION

The Customer will have the ability to request an email is released from quarantine via the email security portal. When this request is triggered, this will be picked up by Softcat's Security Operation Centre, where our highly experienced team of analysts will review the email looking at several key indicators. This will include link analysis, reviewing suspicious attachments for potential malware and utilising threat intelligence to determine if the email requested is safe to release to the recipient. If an email is not deemed to be safe the End-User will receive a declined response with an overview of the reason(s) why.

All users who have items quarantined will receive a daily consolidated quarantine report which will show items quarantined in the last twenty-four (24) hours, where required this can be configured globally to be received at a specific time of day.

Softcat recommend where the Customer utilises Defender O365 that the Customer disables quarantine notifications, this is to prevent End-Users from being able to release emails quarantined by Microsoft without them being triaged first.

2.5 PHISHING REPORTS AND REMEDIATION

Customers will have the ability to report potential phishing emails, when an email has been reported this will be picked up by Softcat's Security Operation Centre where our highly experienced team of analysts will review the email.

An analyst reviewing an email for phishing will examine key indicators such as the sender's address, the tone and content of the message, and any links or attachments. They will assess whether the email contains suspicious elements, such as unexpected requests for sensitive information or poorly crafted content, alongside threat intelligence to determine if it's deemed as phishing. The requesting user will receive confirmation of the outcome. If it's not classified as phishing it could be categorised as spam. Additional policies can be put into place in the form of creating an allow or deny list where required.

2.6 POLICY MANAGEMENT

During onboarding Softcat will setup initial policies in line with known best practice. This will start with the platform being configured in a detect mode, whereby the system monitors emails to detect and log malicious events. But, no remediation action is automatically taken in the case of a malicious email being detected.

This would move onto being configured to prevent (inline) mode, whereby the system inspects all emails and attachments before delivery to users. Malicious items are blocked before reaching users.

All policies can be managed on a user or group level following pre-defined workflows. For example, phishing workflow (quarantine, user is alerted and allowed to request a restore (admin approval required)).

2.7 CHANGE MANAGEMENT

When Softcat makes a recommendation for a critical security patch, a fix, a best practice upgrade or any other recommended change, Softcat and the Customer will follow the Change Management process to implement these changes.

Change Requests, including changes to configuration, will be managed under the Softcat Change Management process with the Customer approving all changes. During the service onboarding process, the Customer will nominate named Customer Contacts who have the authority to approve these changes. The Customer can also initiate a change e.g. a requirement to make a configuration change.

2.7.1 STANDARD CHANGES

Standard changes are pre-approved changes that are determined as carrying extremely low risk. These changes have defined roll out, back out and test plans associated with them. Standard changes will complete within one (1) business day of the request being logged unless the Customer specifies a later date.

2.7.2 NORMAL CHANGES

Normal changes are not pre-approved and will require a Softcat technician to complete a roll out, back out and test plan. Under the Change Management process, these plans will be approved by the Customer, and Change Management approval. If the change is expected to be actioned on a repeated basis, Softcat and the Customer can mutually agree that it is recorded as a standard change.

2.7.3 RETROSPECTIVE CHANGES

Retrospective changes are only permitted if the change was implemented to resolve or immediately prevent an outage on a business-critical system. For a retrospective change to be actioned, the Customer and Softcat Change Management approval will be tracked against the Case of the related issue.

2.7.4 EMERGENCY CHANGES

Emergency changes are raised when the implementation window is required in a time prior to the next available Change Advisory Board meeting (CAB). If a Customer requests an emergency change, then it is implemented entirely at their own risk. If the change is not successful, it will be rolled back, if possible. No ad-hoc trouble shooting will be completed.

2.7.5 CUSTOMER PERFORMED MAINTENANCE

These changes are designed to allow Softcat Support to record when a Customer or a Customer's supplier advises that they are performing maintenance work. These changes they will automatically progress through to an 'Open' and then a 'Closed' state when the scheduled window begins and expires.

2.8 REPORTING

Softcat will configure the platform to provide an automated security checkup report, this is available on a weekly or monthly schedule and is delivered via email. The security checkup report provides a periodic overview of the threats detected in emails and other protected collaboration applications if relevant and configured and how they were handled by the policies in place.

2.9 SERVICE DELIVERY ASSOCIATE

The Service Delivery Management team is a point of contact and escalation for any services detailed within the Work Order. The Service Delivery Management Team is available during standard UK Working Hours.

A named Service Delivery Manager, service report and service reviews are available. Where requested, this will be quoted separately by contacting the Customer's Softcat Account Manager and detailed in the Work Order.

2.10 SIEM INTEGRATION (OPTIONAL ADD-ON)

Softcat can provide support with the integration of the Harmony and Email log forwarding to an external Security Information and Event Management ("SIEM") platform. The current security events that are supported as part of the integration are as follows:

- Phishing
- Suspected phishing
- User reported phishing
- Malware
- Suspected malware
- Malicious URL
- Malicious URL click
- DLP
- Anomaly
- Shadow IT
- Spam

Unless configured otherwise, all events are forwarded over https. As part of the integration all security events get forwarded from a unique static IP for each region, this is dependent on the region where Harmony and Email has been deployed.

This is subject to additional charge which will be quoted separately and detailed in the Work Order.

2.11 EXTENDED ARCHIVING (OPTIONAL ADD-ON)

Archiving options are available up to a maximum of ten (10) years. By default, if this option is taken the archiving is set to seven (7) years and emails will be automatically deleted afterwards.

After activating archiving, all the internal, outgoing and incoming emails (sent or received) from protected users will be archived. For users not licensed for Harmony Email and Collaboration, the emails will not be archived. Emails sent before archiving was activated are not included in the archive.

Harmony Email and Collaboration encrypts and stores the archived emails in the same region as the Customer's Harmony Email and Collaboration tenant in the Infinity Portal.

2.12 SECURITY INCIDENT RESPONSE (OPTIONAL ADD-ON)

Security Incident Response is provided by Softcat's IT Partner, Check Point, and managed by Softcat using the Major Case Management process.

Customers receive twenty (20) hours of Security Event Management as part of the Service. Where Softcat believes an incident would require Security incident Response, the Customer is notified of the recommendation and is asked to confirm their authority to invoke it.

If the Customer has used their twenty (20) hours, additional time can be purchased during the Contract Term. Any additional hours purchased will be confirmed on a Work Order. The Customer is to contact their Softcat Account Manager for more information.

Customers can use their Security incident Response hours for additional Security incident related services from Check Point, such as forensics and threat intelligence.

3. SERVICE LEVELS

3.1 SOFTCAT SUPPORT

Softcat offers a Response Service Level, which is Softcat's commitment to raise a Case within a given time from when the request is made to Softcat Support.

In the table below, the Service Level column is the percentage of requests responded to within the Response Service Level metric, for example: 95% of Cases logged as a P1 are responded to within fifteen (15) minutes.

Softcat offers a resolution Service Level, which is Softcat's commitment to resolve a Case through Fix or workaround.

The Response metrics for Cases are shown in the table below:

Priority	Description	Service coverage hours	Response metric	Notification method	Service Level target
Priority 1 (P1)	Business impacted or imminent impact expected within four (4) hours; full Customer Site outage; a business-critical system or Supported Product is not working; Customer cannot perform business critical functions; loss of revenue; risk of severe reputational damage; all end-users unable to perform business critical roles.	24/7	<15 Minutes	Phone call and Email	95%
Priority 2 (P2)	Partial Customer Site outage; loss of redundancy; a non-business-critical system or Supported Product is down; Customer experiencing a high degradation in Service; risk to revenue generation; multiple End-Users unable to perform business critical roles.	24/7	<30 Minutes	Email	95%
Priority 3 (P3)	Single End-User issue that prevents them from performing business-critical elements of their role; multiple End-Users affected by an identical issue that	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	Email	95%

	does not prevent them from performing their roles; reduction in redundancy for business-critical systems.				
Priority 4 (P4)	Single user issue that does not prevent them from performing their role or a critical operation; reduction in redundancy for non-business critical systems.	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	Email	95%

Category type	Description	Service coverage hours	Response metric	Fulfilment target	Service Level target
Request [3]	Request – Working Hours only	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	5 Working Days	95%

3 Unless specified otherwise, any requests are subject to the above metrics.

3.2 CHANGE MANAGEMENT

The Service Level is determined by the type of change. The Service Level starts from when the Customer supplies Softcat with all of the information that is required by Softcat for the completion of the work. Any time spent determining the Customers' expectations or requirements will not be included in the Service Level.

Category type	Description	Service coverage hours	Response metric	Fulfilment target	Service level target
Standard change	A pre-approved procedural change with minimum risk and impact to service. [4]	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	1 Working Day	95%
Normal Change	A change, which requires authorisation, is complex and / or requires down time for a related service.	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	5 Working Days [5]	95%
Emergency Change [6]	A change required to restore service or protect / mitigate a threat to the environment where it is not acceptable to restore	Applied in line with a Major Case (Priority 1)			

	under the related Incident case.	

[4] This is dependent on all required information being received to complete the request.

[5] Dependent on complexity, impact and approved design.

[6] Softcat reserve the right to disable users, services or devices, which are found to present an immediate threat to the Customer or Softcat environment without authorisation. This also excludes project related tasks where scope has deviated from agreed design.

4. CUSTOMER RESPONSIBILITIES

4.1 SOFTCAT SUPPORT

a. The Customer should ensure that Customer Contacts are skilled in or knowledgeable of the Customer's Operating Environment, have sufficient access rights and be of a sufficient proficiency to apply the recommendations that are provided as part of this service
b. Prior to Service commencement the Customer should provide:
    i. A minimum of two (2) Customer Contacts for the purpose of support and continuity.
    ii. Any relevant Key Information e.g. models, serials, tenancy, subscription
c. When raising a Case the Customer Contact should provide, when requested by Softcat:
    i. Reasonable visibility of system logs, configuration files and error messages
    ii. A description of the symptoms and other devices or services impacted
    iii. Confirmation when the issue first occurred and if it has occurred before (where possible provide previous Case references)
    iv. Details of any recent changes or projects implemented prior to the issue being raised
    v. Details of all attempted fixes, configuration amendments and updates performed already to attempt to resolve prior to raising the Case or Request
    vi. To what extent the issue is affecting operation of the Customer's business
    vii. The number of End-Users impacted and their location
    viii. Contact details of the Customer Contact
d. Implementation of best practice recommendations advised by Softcat
e. Direct support for End-Users. Customers should ensure the Customer's staff are trained to refer all Cases to the Customer Contact in the first instance, and not permit persons other than a Customer Contact to approach Softcat to register a Case
f. Provide thirty (30) days' notice to Softcat of any requested addition(s) to the Supported Product list
g. Follow the information in the "Softcat Services Welcome Pack"
h. Use the service only for the business purposes of the Customer and keep all access credentials and certificates, which Softcat may provide to allow access to the service, safe and secure, and not share them with any third party without Softcat's prior written consent
i. Not use or attempt to use or misuse the Services in any way that is criminal or otherwise unlawful in any relevant jurisdiction

4.2 PLATFORM

a. The Customer is responsible to ensure their license count and license applied are done correctly. This includes taking into consideration any additional licences required throughout the duration of the service with any joiners, movers and leavers ("JML")
b. To ensure in readiness for onboarding they have access to a user with Microsoft Global Administrator permissions to accept the applicable application registration

4.3 ANTI-PHISHING and MALWARE PROTECTION

To prevent outgoing emails from failing SPF checks and being quarantined, the Customer is required to add the following to their SPF records: include:spfa.cpmails.com

4.4 QUARANTINE MANAGEMENT AND REMEDIATION

a. To ensure that End-Users utilise the email security portal for requesting any emails being released from quarantine.
b. Softcat recommend where the Customer utilises Defender O365 that the customer disables quarantine notifications, this is to prevent End-Users from being able to release emails quarantined by Microsoft without them being triaged first.
c. To ensure that their users are adequately trained on the best practices for using the relevant portal(s) and are aware of potential security threats, such as phishing attacks.

4.5 CHANGE MANAGEMENT

Customer has a responsibility to ensure that their Authorised Contact List is maintained accurately. This determines who is a change approver and who is a commercial approver.

4.6 REPORTING

To ensure we're notified of any amendments required to the recipient list of the automated reports.

4.7 SERVICE DELIVERY ASSOCIATE

a. Keep Customer contacts up to date to allow Service Delivery Associates to provide the Service effectively.
b. Provide advanced notification to Softcat Support of any planned maintenance that could have an impact on any hardware or Software that Softcat provide Services for.
c. Provide advanced notification to Softcat Support of any planned decommissioning of Softcat related equipment or Software.

4.8 EXTENDED ARCHIVING (OPTIONAL ADD-ON)

To ensure if required they export all relevant emails from the archive in advance of the Service terminating.
The Customer must have an active licence to access any archived material.

5. NOTABLE EXCLUSIONS

5.1 SOFTCAT SUPPORT

a. At an additional cost the Customer can request project and design work, including Professional Services by contacting their Account Manager for a quote.

5.2 SERVICE DELIVERY ASSOCIATE

a. Any reporting or service reviews. [7]
b. Service Delivery Associates will not act as a project manager or in any other capacity outside of the activities described in this Service Description.

[7] This is available, but subject to an additional charge. Customers can request a quote by contacting their Softcat Account Manager.

6. SERVICE ACCEPTANCE AND ONBOARDING

Following receipt of a Customer purchase order, Softcat will confirm the Contract by sending a Work Order, which is usually undertaken online via DocuSign.

Following the acceptance of the Contract, the Onboarding Period will begin. This is the period in which any pre-requisite dependencies for the Service are completed, for example the collation of the Key Information. If there is a requirement for any additional assessment of the Customer's Operating Environment following Softcat's receipt of the Key Information, this will be undertaken during the Onboarding Period.

At the end of the Onboarding Period, the Customer will be provided with an Acceptance Into Service (AIS) document which is required to be signed by the Customer within five (5) days of receipt. The Activation Date for the Service will be the day on which the Onboarding Period ends and is signed off as complete by the Customer or, in the event of no response, five (5) days after the Onboarding Period has completed and the AIS document has been provided (which is the sooner). Where any Key Information requested by Softcat is outstanding at the Activation Date, Softcat's obligation to deliver the Service shall be subject to reasonable endeavours.

Shortly after the Work Order is sent, the Customer will receive a "Softcat Services Welcome Pack" document, which includes key contact details for Softcat, an overview of the escalation process, and other useful information.

7. SERVICE BILLING AND CONTRACT TERM

The billing frequency, Contract Start Date and the Initial Term will be agreed with the Customer and confirmed in the Work Order.

Unless it is stated on the Work Order that the Service will not Auto-Renew, or written notice is given by either Party to the other of its intention not to renew the Contract at least ninety (90) Working Days before the expiry of the Initial Term or any subsequent Renewal Term, the Service at the expiry of the Initial Term or any subsequent Renewal Term will be renewed automatically for a further term of twelve (12) months on the same Terms and Conditions as detailed within the Contract.

8. TERMS AND CONDITIONS

8.1 OVERVIEW OF TERMS AND CONDITIONS

The delivery of the Service to the Customer shall be governed by Softcat's Terms and conditions, this Service Description and the Work Order, and the other Agreements listed below.

- Softcat terms and conditions: https://www.softcat.com/terms-and-conditions-uk/
- Check Point Incident Response SLA: https://www.softcat.com/documents/incident-response.pdf

Capitalised terms in this document shall have the meaning set out here: https://www.softcat.com/documents/glossary-and-definition-of-terms.pdf, unless they are defined in the Terms and Conditions.

In the Event of any discrepancy or conflict between the Softcat T&Cs, this Service Description and the Work Order, the Work Order shall take precedence to the extent of any discrepancy or conflict.

For the purposes of the relevant Work Order and this Service Description, the Term "Service" shall be interpreted as an "Annuity Service".

8.2 DATA PROCESSING AGREEMENT AND ACCEPTANCE OF THE CONTRACT

By signing the Work Order, the Customer agrees to the Data Processing Agreement (DPA), available here: https://www.softcat.com/documents/Softcat-Services-DPA2019.pdf

The DPA shall be a separate Agreement to the Contract (and no liability shall arise (i) under this Contract in respect of the Processing, or (ii) under the Processing Agreement in respect of the remaining aspects of providing or using the Annuity Services).

If, in the absence of a signed Work Order but following receipt of this Service Description, the Customer provides a PO for the Services and/or instructs Softcat to provide the Services, the Customer shall be deemed to have accepted the terms and conditions of the Contract, including the Service Description and the DPA.

8.3 ADDITIONAL TERMS

8.3.1 SECURITY INCIDENT RESPONSE

Softcat plc (Softcat) has agreed to arrange the supply to the Customer (as named in the signature block below) certain managed or ongoing services ("Managed Services"), subject to the Softcat Terms and Conditions (current version available at https://www.softcat.com/terms-and-conditions-uk/ and on request, and capitalised Terms in this document which are not defined here shall be interpreted in line with the Terms and Conditions).

Softcat has sub-contracted the provision of the Supplies to its subcontractor (IT Partner), who has provided details of the Service by way of a Service Description (https://www.softcat.com/documents/incident-response.pdf).

Pursuant to this document, the Check Point Incident Response Service Level Agreement shall be considered part of the Agreement between Softcat and the Customer.

In the Service Description noted in the Security Incident Response section, if there is reference to Softcat as the party the IT Partner is delivering to, this shall be interpreted as referring to the Customer and, correspondingly, where in that document there is reference to the IT Partner, this shall be interpreted as referring to Softcat, so that the effect is that Softcat and the Customer have the same rights, entitlement, duties and obligations to each other under the Agreement as would be the case between the IT Partner and Softcat (respectively) under the Service Description.

By signing the Work Order, Softcat and the Customer agree to the above and the contents of the Service Description.

8.4 ISO STANDARDS

The Service is fully compliant with the following ISO standards, ensuring the highest levels of quality, security and continuity:

- **ISO 20000** – Focuses on IT service management, ensuring that service are aligned with business needs and adhere to best practices. By following ISO 20000, the Service guarantees that the IT service management processes are efficient, effective, and continually improving to meet Customer evolving demands.
- **ISO 27001** – Dedicated to information security management systems. It helps organisations protect data and manage security risks systematically. Compliance with ISO 27001 ensures that robust security measures are in place to safeguard sensitive information, mitigate risks and respond promptly to security Incidents.
- **ISO 9001** – Addresses quality management systems. It ensures that the Service consistently meets Customer requirements and strives for continuous improvement. By adhering to ISO 9001, the Service demonstrates commitment to delivering high-quality services that enhance Customer satisfaction and operational excellence.
- **ISO 22301** – For business continuity management systems, helping organisations prepare for a respond to disruptive Incidents. Compliance with ISO 22301 ensures that the Service has comprehensive plans and procedures in place to maintain business operations during unforeseen events, thereby minimising downtime and ensuring service continuity.

SOFTCAT PLC, FIELDHOUSE LANE, MARLOW, BUCKS, SL7 1LW