Computing Dynamics Limited

Schedule 2: Managed Cyber Security

Version 2026.11.2

Issued 24 November 2026

This Schedule applies where a customer's Order includes Managed Cyber Security. It forms part of the Agreement and is read with the General Terms, where the capitalised terms used here are defined. Prices, the plan chosen and the length of the agreement are set out in the Order. What each plan includes is set out in the Service Description in the Annex.

Please note in particular clause 6 (length of the agreement and renewal), clause 8 (action taken without prior approval during a security incident, and chargeable time), clause 12 (limits of the service) and clause 13 (charges for ending early).

Part A: The service

1. Definitions

1.1 In this Schedule:

Add-on means an optional security service listed as an add-on in the Order.

Committed Term means the Initial Term or the current Renewal Term.

Device means a computer or server on which Computing Dynamics' management software is installed and active.

Plan means the Core, Complete or Device-only plan stated in the Order.

Security Incident means an actual or suspected compromise of, or attack on, the Customer's accounts, Devices or data that is detected by the Service or reported by the Customer. Events that have the same cause, such as one compromise that affects several accounts or continues over several days, are one Security Incident.

Security Operations Centre means the third-party service that monitors alerts from the Service at all hours.

Service means the Managed Cyber Security supplied to the Customer under this Schedule, consisting of the Plan and any Add-ons in the Order.

Service Description means the description of the Plans and Add-ons in the Annex to this Schedule.

User means a user account in the Customer's Microsoft 365 tenant that holds a paid licence, including a licensed shared or generic mailbox.

Waived Charges means one-off charges that Computing Dynamics has waived under clause 5.3.

2. The Service

2.1 Computing Dynamics will supply the Plan and any Add-ons stated in the Order. The components of each Plan and Add-on are described in the Service Description.

2.2 An Add-on is available only with the Core or Complete Plan.

2.3 The Device-only Plan covers Devices only. It does not include protection for email, user accounts or Microsoft 365 data, or any backup.

2.4 The Service protects only the Users and Devices counted under clause 4. A computer or server without Computing Dynamics' management software, and an account outside the Customer's Microsoft 365 tenant, is not covered.

2.5 The Service is a security service. It does not include general IT support, which is available through Pre-Paid Support or Managed Support.

2.6 The Service Description forms part of this Schedule and may be changed in the same way, under clause 23 of the General Terms.

3. What the Customer needs to have in place

3.1 Except on the Device-only Plan, the Customer needs a Microsoft 365 tenant with licences that support the components of its Plan. Computing Dynamics will tell the Customer before the Start Date if its licences do not.

3.2 The Customer will: (a) give Computing Dynamics the administrative access to its Microsoft 365 tenant and Devices that the Service needs; (b) tell Computing Dynamics about every computer and server used for its business, so that the management software can be installed; (c) keep Devices on operating systems that are within their manufacturer's support period, and connected to the internet often enough to receive updates; and (d) make sure its users complete the security awareness training provided.

3.3 If these requirements are not met, parts of the Service may not work as intended. The Fees remain payable, and clause 6.4 of the General Terms applies.

4. Users, Devices and Fees

4.1 The Fees are charged each month at the prices in the Order, as follows: (a) the user price for each User, which includes one Device; (b) the additional user price, in place of the user price, for each User in excess of the number of Devices, being a User who shares a Device that is already covered or who has no Device; and (c) the additional device price for each Device in excess of the number of Users. A server is a Device.

4.2 A User or Device is covered and charged from the date it is added, pro-rated for that month, without a further Order. One that is removed is charged to the end of the month in which it is removed. A User is added when a licence is assigned to the account and removed when the licence is removed; a Device is added when Computing Dynamics' management software is installed on it and removed when that software is removed. Computing Dynamics checks the numbers each month against licence and management records. Where the check shows a change that has not been reflected in the Fees, Computing Dynamics will correct the Fees from the date of the change, whether the correction is up or down, for up to the previous 12 months.

4.3 An account stops being a User when its licence is removed. The Customer is responsible for telling Computing Dynamics when a user leaves so that the licence can be removed. Because the prices in clause 4.1 depend on the numbers of Users and Devices, the price that applies to a User can change when either number changes.

4.4 Where Users cannot be measured, for example at a site with shared computers or without Microsoft 365, the Order may state that the Fees are calculated on Devices.

4.5 The Order may state a minimum number of Users and Devices. Where it does, the number of Users and the number of Devices used to calculate the Fees under clause 4.1 are each the actual number or the minimum, whichever is greater.

5. One-off charges

5.1 The onboarding charge stated in the Order is payable when the Order is accepted.

5.2 Where the Customer adds an Add-on or moves to a higher Plan after the Start Date, a one-off charge equal to one month's Fees for what is added is payable, as stated in the quotation for the addition.

5.3 Where the Initial Term is 36 months: (a) the onboarding charge is waived; and (b) the charge under clause 5.2 is waived if at least 12 months of the Initial Term remain on the date the addition starts, or if the Customer agrees a new 36-month term at the same time.

5.4 Waived Charges become repayable if the Service ends early, as set out in clause 13.

Part B: Term and price

6. Length of the agreement and renewal

6.1 The Initial Term is 12 months or 36 months from the Start Date, as stated in the Order.

6.2 At the end of the Initial Term, and of each Renewal Term, the Service renews for a further Renewal Term of 12 months, unless either party has given the other at least 30 days' written notice before the end of the current term that it does not wish to renew.

6.3 A further 36-month term is agreed by a new Order. Computing Dynamics aims to send a renewal proposal about 90 days before the end of a 36-month Initial Term.

6.4 The benefits of a 36-month term in clauses 5.3, 7.2 and 11.4 apply during a 36-month Initial Term only. They do not apply during a 12-month Renewal Term.

6.5 An Add-on or Plan change made during a Committed Term ends on the same date as the rest of the Service.

6.6 The Customer may add an Add-on or move to a higher Plan at any time. It may remove an Add-on or move to a lower Plan only from the end of the Committed Term, on at least 30 days' written notice.

7. Price changes

7.1 During a 12-month Initial Term and any Renewal Term, clause 9 of the General Terms applies.

7.2 During a 36-month Initial Term, clauses 9.1 to 9.3 of the General Terms do not apply to the recurring prices in the Order. Instead, Computing Dynamics may increase those prices once a year, with effect from an anniversary of the Start Date, by a percentage no greater than the lower of: (a) the annual rate of increase in the UK Consumer Prices Index published for the month that falls two months before that anniversary; and (b) 6%.

7.3 Computing Dynamics will give at least 30 days' written notice of an increase under clause 7.2. An increase that is not taken in one year cannot be added to a later year.

7.4 Clauses 9.5 and 9.6 of the General Terms, on resold licences and changes in numbers, apply throughout. The Charges, including hourly rates and fixed charges, continue to change under clause 9.1 of the General Terms.

Part C: How the service works

8. Security Incidents

8.1 The Security Operations Centre monitors the components of the Service that the Service Description states are monitored at all hours.

8.2 The Customer authorises the Security Operations Centre and Computing Dynamics to act immediately, without asking first, to contain a Security Incident. This may include isolating a Device from the network, locking or disabling an account, ending sessions, resetting credentials and blocking a file, process or email.

8.3 Containment may interrupt the Customer's work. Computing Dynamics is not liable for interruption caused by containment action taken in good faith, including where the alert later proves to be a false alarm.

8.4 Computing Dynamics will tell the Customer's main contact about a Security Incident as soon as it reasonably can, and will investigate and help the Customer recover during Standard Hours. Work outside Standard Hours is at Computing Dynamics' discretion and is charged as out-of-hours work under the Charges.

8.5 Computing Dynamics' time on a Security Incident is chargeable under clause 10 of the General Terms. So that work can start without delay, the first 30 minutes on each Security Incident are approved in advance by the Customer. Further work will be agreed with the Customer first.

8.6 Chargeable time is deducted from the Customer's Pre-Paid Support balance if it has one, and is otherwise charged at the Ad Hoc Rate. Where the Customer also has Managed Support, Schedule 3 sets out the time that is included.

8.7 The Customer will report any suspected Security Incident to Computing Dynamics promptly, co-operate in dealing with it, and notify its own insurer where required. Decisions on reporting an incident to a regulator, or to the people affected, are the Customer's, with the help described in the Data Processing Addendum.

8.8 The Service is not a full incident response service. Forensic investigation, legal advice, regulatory notifications, public relations and dealing with those responsible for an attack are not included. Computing Dynamics will work with specialists appointed by the Customer or its insurer, and that time is chargeable.

9. Third-party providers

9.1 The Service is delivered using Third-Party Services, including the Security Operations Centre. Clause 5 of the General Terms applies to them, and the providers that process personal data are named in Computing Dynamics' sub-processor list.

9.2 Detection relies on the providers' own threat information and detection methods, which change over time and are outside Computing Dynamics' control.

10. Backup

10.1 Managed 365 Backup covers the Microsoft 365 data described in the Service Description. It does not cover data held on Devices or in other applications.

10.2 Backups run at the frequency, and are kept for the periods, stated in the Service Description. Backup history is kept for as long as the Service continues on the same backup platform.

10.3 When the Customer tells Computing Dynamics that a user has left, Computing Dynamics will normally convert that user's mailbox to a shared mailbox, which continues to be backed up. If the Customer asks for the account to be deleted instead, the backup history for that account is deleted 30 days after the account is deleted, unless the Customer asks in writing before then for it to be kept. A monthly charge, quoted by Computing Dynamics, applies to backup history kept for a deleted account.

10.4 If Computing Dynamics moves the Service to a different backup platform, it will give the Customer at least 60 days' written notice. Backup history cannot be moved between platforms. The history held on the previous platform is deleted when that platform is retired, unless before then the Customer asks for an export, which is chargeable, or agrees to pay the cost of keeping it. A change of backup platform is a change to which clause 23.2 of the General Terms applies.

10.5 Where the Order includes a server or workstation backup Add-on, the Order states what is backed up, how often and for how long, for each server or computer. Any backup equipment supplied for the Add-on remains the property of Computing Dynamics or its supplier and must be returned when the Add-on ends.

10.6 Computing Dynamics monitors whether backups have completed and will investigate failures. Where the Customer has Managed Support, restoring data at its request is included as set out in Schedule 3. Otherwise it is additional work under clause 10 of the General Terms.

10.7 When the Service ends, the backup data is deleted as described in clause 21.5 of the General Terms. The Customer must ask for any export it needs before the end date.

11. Reviews, training and Cyber Essentials

11.1 Where the Service includes security reviews, Computing Dynamics will carry them out as described in the Service Description, including any improvement work up to the time stated there. Work beyond that time is chargeable under clause 10 of the General Terms.

11.2 Where the Service includes security awareness training and simulated phishing emails, Computing Dynamics will share the results with the Customer's main contact. The Customer is responsible for its users taking part.

11.3 Help with Cyber Essentials certification is not part of a Plan. Where the Customer asks for it, the certification fee stated in Computing Dynamics' quotation is payable and Computing Dynamics' time is chargeable under clause 10 of the General Terms. Certification is decided by the certification body and is not guaranteed.

11.4 On the Complete Plan with a 36-month Initial Term, the following are included once in each year of that term: (a) the certification fee; and (b) up to three hours of Computing Dynamics' time to complete and submit the assessment. Time beyond three hours is chargeable.

11.5 Work needed to bring the Customer's systems up to the Cyber Essentials standard is not included in any case and is quoted separately.

12. Limits of the Service

12.1 The Service is designed to reduce the likelihood of a Security Incident and to limit its effect. As clause 16.1 of the General Terms states, no security service can prevent or detect every attack.

12.2 The Service is not insurance. Computing Dynamics recommends that the Customer holds cyber insurance. The Service does not by itself satisfy the conditions of any insurance policy, and the Customer is responsible for checking what its insurer requires.

12.3 Computing Dynamics is not responsible for a Security Incident to the extent that it results from: (a) a computer, server, account or system that is not covered by the Service; (b) the Customer or its users removing, disabling or bypassing a security control; (c) a Recommendation that the Customer has declined; or (d) the Customer or its users sharing credentials or approving a fraudulent sign-in or payment request.

Part D: Ending the service

13. Ending the Service early

13.1 The Customer may end the Service before the end of a Committed Term by giving at least 30 days' written notice. If it does so, the charges in this clause are payable.

13.2 The early termination charge is 75% of the Fees that would have been payable for the Service from the date it ends to the end of the Committed Term. It is calculated on the average monthly Fees for the Service over the three months before notice of termination was given by either party.

13.3 In addition, Waived Charges are repayable in the following proportion: (a) for the onboarding charge, the part of the 36-month Initial Term that remains on the date the Service ends, divided by 36 months; and (b) for a charge waived on a later addition, the part of the term that remains on the date the Service ends, divided by the period from the date the addition started to the end of the term.

13.4 Where Cyber Essentials certification was included under clause 11.4, the certification fee for any certification completed in the 12 months before the date the Service ends is also repayable, at the fee that would have been payable under clause 11.3.

13.5 The early termination charge does not include the Fees for resold licences and subscriptions, which remain payable under clause 5.5 of the General Terms.

13.6 The charges in this clause are also payable where Computing Dynamics ends the Service under clause 20.2, 20.3 or 20.4 of the General Terms. They are not payable in the cases listed in clause 20.6 of the General Terms.

13.7 The Customer accepts that Computing Dynamics commits to its own suppliers for the Committed Term and prices the Service on that basis, and that the charges in this clause are a fair price for ending early.

14. When the Service ends

14.1 When the Service ends, Computing Dynamics will remove its software from the Devices, and monitoring, protection, backup and the Add-ons will stop. Clauses 12.3 and 21 of the General Terms apply.

14.2 The Customer is responsible for exporting any data it holds in an Add-on, such as a password manager, before the end date, and for putting alternative protection in place.

Annex: Service Description

A1. Core Plan

Each User is covered by the following. The components that protect a Device apply to each Device covered under clause 4.

Managed Email Security: checks incoming email for phishing, impersonation and harmful links or attachments.

Managed 365 Backup: an independent backup of Microsoft 365 data, as described in A5.

Managed Security Awareness Training: regular online training and simulated phishing emails for each User.

Managed Dark Web Monitoring: alerts when the Customer's email addresses and passwords appear in known data breaches.

Managed Identity Threat Detection: monitoring of the Customer's Microsoft 365 accounts for signs of unauthorised access, with action to contain a compromised account. Monitored at all hours by the Security Operations Centre.

Managed Patching: operating system and common application updates on each Device.

Managed Threat Detection: protection of each Device against ransomware and other threats. Monitored at all hours by the Security Operations Centre.

A2. Complete Plan

Everything in the Core Plan, and the following. Each is also available as an Add-on to the Core Plan.

Managed Account Security: continuous checking of the Customer's Microsoft 365 security settings against a hardened baseline, with alerts when a setting changes.

Managed Web Protection: blocking of harmful and unsuitable websites, reporting of unapproved cloud applications and control over the use of AI tools.

Managed Password Security: a business password manager for each User.

Managed Admin Rights: removal of the need for users to hold administrator rights on their Devices, with approved software installations handled on request.

Managed Security Reviews: a monthly review of the Customer's Microsoft 365 security settings with up to 30 minutes of improvement work each month; a monthly external vulnerability scan with a report of findings; an annual cyber security review; and a written incident response plan.

A3. Device-only Plan and additional Devices

Device-only Plan: Managed Patching and Managed Threat Detection for each Device.

Additional user: all the components of the Plan that protect a User and their account, for a User who shares a Device that is already covered or who has no Device.

Additional Device on the Core Plan: Managed Patching and Managed Threat Detection.

Additional Device on the Complete Plan: Managed Patching, Managed Threat Detection and Managed Admin Rights.

A4. Other Add-ons

Workstation Image Backup and Server Backup: backup of an individual computer or server, with the scope, frequency and retention stated in the Order.

Cyber Essentials: help with certification, charged as set out in clause 11.3, or included to the extent set out in clause 11.4.

A5. Managed 365 Backup

Data covered: Exchange Online mailboxes (mail, calendar, contacts and tasks), OneDrive, SharePoint sites and Teams data, for each User and for the shared mailboxes that Computing Dynamics has added to the backup.

Frequency: up to three times a day.

Retention: every backup is kept for 30 days. After 30 days, one backup a day is kept. After 90 days, one backup a week is kept. After one year, one backup a month is kept, for as long as the Service continues on the same backup platform.