Cybersecurity Services Schedule

Centra Networks Pty Ltd (ACN 107 228 937)

Last updated: 24 March 2026

1. About this Service Schedule

1.1. This Service Schedule only applies where an Order expressly provides for our supply of one or more of the following services to you:
(a) Cybersecurity Hardware;
(b) Cybersecurity Software;
(c) Endpoint Security Management Services;
(d) Cybersecurity Consulting Services;
(e) Managed Cybersecurity Services.

1.2. This Service Schedule must be read in conjunction with our Terms of Service executed between you and us and the other documents that comprise an Agreement.

2. Cybersecurity Hardware and Software

2.1. This clause Error: Reference source not found only applies where an Order provides for our supply to you of Third Party Security Products.

2.2. The Third Party Security Products will provide you with access to security hardware and/or software (as applicable) that will be made available to you for you to use at the Site or in a hosted environment, as set out in the Order.

2.3. Where expressly specified in the Order, we will configure the Third Party Security Products or configure other Products and Services (including by applying security settings or installing additional cybersecurity components, software or tools to them) in accordance with the requirements of the Order.

2.4. If we provide you with recommendations concerning which Third Party Security Products to purchase, we do not represent that the Third Party Security Products will prevent or block all security attacks to your networks, computer systems and environment.

2.5. It is your sole responsibility to select the Third Party Security Products and associated configuration options that are most appropriate for your cybersecurity needs and unless the Order provides for us to carry out a full audit of your IT environment, you warrant to us that you have conducted all investigations and made all necessary inquiries in order to satisfy this requirement.

2.6. Our provision of Third Party Security Products may be subject to a service level agreement or other Vendor Terms published by the Third Party Provider of the Third Party Security Products from time to time.

2.7. You agree to use, and ensure that your End Users use, Third Party Security Products only in accordance with the relevant Agreement and any applicable Vendor Terms.

2.8. Vendor Terms will, among other things, grant you a right to use the Third Party Security Products and specify associated obligations. The Vendor Terms may be detailed in a licence issued by the Vendor and will be appended to or referred to in the relevant Order that we issue to you for the Third Party Security Products or otherwise available from us upon request.

2.9. You acknowledge that the Third Party Security Products may be unavailable at times, due to various factors including network maintenance, peak congestion or failure of Your Equipment. You further acknowledge that other than in respect of guarantees that may be implied in the relevant Agreement under the ACL or other non-excludable Applicable Law, we do not guarantee the speed, performance or quality of the Third Party Security Products, although certain credits or rebates may be available under applicable Vendor Terms. Where such credits or rebates are available and provided to us for Third Party Security Products that we supply to you, we will pass on those credits or rebates to you on a pro rata basis.

2.10. Emergency maintenance and scheduled maintenance in relation to Third Party Security Products may be required from time to time. Should this be necessary, we will provide as much notice as is reasonably practicable and where within our control, we will endeavour to conduct such maintenance at times that are unlikely to impact most clients.

2.11. Fees for Third Party Security Products may include establishment, monthly recurring (which may be invoiced in advance), usage-based and other associated charges (including for hardware, software and professional services). All such Fees are set out in the Order.

2.12. If there is a data allowance associated with a particular Third Party Security Product and it is not used within the period for which it is provided, it does not roll-over into a subsequent period.

2.13. You acknowledge that devices connected to a network, and particularly but not limited to those connected to the Internet, are subject to security threats and other than in respect of guarantees that may be implied in the relevant Agreement under the ACL or other non-excludable Applicable Law, no representation, warranty or guarantee is provided that Third Party Security Products or other Products and Services will be able to completely eliminate all or any specific types of security vulnerabilities or threats on your network.

2.14. Without limiting clause Error: Reference source not found above (and without making any warranty or representation), we recommend that you take up all appropriate options within the Third Party Security Products and employ other security technologies in conjunction with the Third Party Security Products to reduce your risk of an information technology security incident.

2.15. If you experience a fault that you consider is with a Third Party Security Product, you must use reasonable endeavours to determine if the fault is caused by Your Equipment or otherwise within your responsibility, prior to contacting us for support. Should you request after-hours support and the fault is found not to be related to a Third Party Security Product, we may impose a professional service fee at our then current rates for the time we spent communicating with you about the fault and investigating it. In any event, support for Third Party Security Products is only available if you enter into an agreement that provides for our provision of support services in respect of the Third Party Security Products in accordance with our Managed Services Service Schedule.

2.16. Any consulting services that you require in connection with a Third Party Security Product will be subject to our Professional Services Service Schedule.

3. Endpoint Security Management Services

3.1. If "*Endpoint Security Management Services*" is specified in an Order (**Security Endpoint Management Services**), we will during the Term of the relevant Agreement:

(a) read and respond to any security notifications issued to us with respect to potential security issues reported by security management software that we install on any items expressly specified in an Order as being covered by Security Endpoint Management Services (**Monitored Items**); and

(b) install security updates and other software patches to the Monitored Items after receiving notice of the existence of the updates and patches where they are available to us free of charge or paid for by you.

4. Cybersecurity Consulting Services

4.1. If "Cybersecurity *Consulting Services*" is specified in an Order, we will provide the consulting services in accordance with any requirements set out in the Order (**Cybersecurity Consulting Services**).

4.2. The Cybersecurity Consulting Services will be limited to recommendations about Third Party Security Products.

4.3. Although we will provide recommendations concerning which Third Party Security Products to purchase as part of the Cybersecurity Consulting Services, we do not represent that the Third Party Security Products will prevent or block all security attacks to your networks, computer systems and environment.

4.4. Our Fees for the Cybersecurity Consulting Services will be charged in the same manner as Professional Services as set out in clause 2 of our Professional Services Service Schedule, which is available from us upon request.

5. Managed Cybersecurity Services

5.1. If "*Managed Cybersecurity Services*" are specified in an Order (**Managed Cybersecurity Services**):

(a) we will deploy firewalls and other security products that are designed to maintain your network security (but only to the extent those firewalls and products are specified in the Order);

(b) we will use our best endeavours to identify security breaches, threats and vulnerabilities on the devices or networks specified in the Order as being covered by the Managed Cybersecurity Services (in this clause 5, **Your Devices and Networks**);

(c) you acknowledge that devices connected to Your Devices and Networks, particularly but not limited to those connected to the internet, are subject to security threats and that although our Managed Cybersecurity Services are designed to reduce certain types of security breaches, threats and vulnerabilities specified in the Order, no representation, warranty or guarantee has been provided that our Managed Cybersecurity Services will definitely be able to identify or eliminate all or any specific types of security breaches of, and threats or vulnerabilities to, Your Devices and Networks.

6. Cybersecurity Risk and Compliance Services - Essential Eight

6.1. If "*Cybersecurity Risk and Compliance Services - Essential Eight*" are specified in an Order, we will provide these services in accordance with the scope and requirements set out in that Order (**Essential Eight Services**), subject to the relevant Agreement.

6.2. The Essential Eight Services will be delivered using the Ordered Products and Services, which may or may not include Third Party Security Products, as specified in the Order and will focus on supporting your implementation of the Australian Cyber Security Centre's (ACSC) Essential Eight Maturity Level 1 (E8 ML1) strategies in respect of the devices or networks specified in the Order as being covered by the Essential Eight Services (in this clause 6, **Your Devices and Networks**).

6.3. The Essential Eight Services will include the following activities during the Term, in respect of Your Devices and Networks:

(a) continuous scanning of Your Devices and Networks to assess alignment with E8 ML1 controls;

(b) risk management dashboarding and visualisation to track compliance gaps and mitigation activities;

(c) automated and manual data collection from external sources to support compliance assessments;

(d) reporting of progress against E8 ML1 across all eight mitigation strategies;

(e) quarterly compliance reviews to assess alignment with your business's technology roadmap and evolving risk profile;

(f) continuous compliance monitoring to identify control drift or configuration changes;
(g) ongoing risk identification, prioritisation and tracking aligned to the Essential Eight framework; and
(h) regular updates to the Compliance Manager GRC platform reflecting changes in control requirements, system configurations and baseline settings relevant to E8 ML1.

6.4. While we will take reasonable steps to support your compliance with E8 ML1 through the Essential Eight Services:
(a) ultimate responsibility for compliance with Applicable Laws, standards and frameworks remains with you;
(b) we do not guarantee that your organisation will achieve or maintain compliance or eliminate all or any specific cybersecurity risks whether as part of the Essential Eight Services or otherwise; and
(c) compliance outcomes are dependent on various factors, including your internal processes, systems and responsiveness to identified issues.

6.5. Our Fees for the Essential Eight Services will be charged in accordance with the applicable Order.

7. Definitions and Interpretation

7.1.[6.1.] In this Service Schedule, words in bold font in parentheses have the meanings given to them therein and words starting with a capital letter in this Service Schedule that are not otherwise defined in this Service Schedule have the meanings given to them in the Terms of Service. In addition, the following words have the following meanings:

Third Party Security Products means the security hardware and/or software products specified in an Order.

Vendor Terms means a Third Party Provider's terms and conditions, as detailed in a licence agreement, end user agreement, terms of service or other similar customer agreement, issued by the Third Party Provider and referred to in or appended to an Order (or that is available from us on request) for Third Party Security Products.