EXPOSURE DRAFT

Cyber Security (Security Standards for Smart Devices) Rules 2024

I, Tony Burke, Minister for Home Affairs, make the following rules.

Dated 2024

Tony Burke **[DRAFT ONLY—NOT FOR SIGNATURE]**
Minister for Home Affairs

Contents

Part 1—Preliminary

1 Name

This instrument is the *Cyber Security (Security Standards for Smart Devices) Rules 2024*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information	
Column 3	
Date/Details	
1. Part 1 and anything in this instrument not elsewhere covered by this table	The day after this instrument is registered.
2. Part 2	The day after the end of the period of 12 months beginning on the day Part 2 of the *Cyber Security Act 2024* commences.
3. Schedule 1	At the same time as the provisions covered by table item 2.

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under the *Cyber Security Act 2024*.

4 Definitions

Note: A number of expressions used in this instrument are defined in the Act, including the following:

(a) manufacturer;

(b) relevant connectable product;

(c) supplier.

In this instrument:

Act means the *Cyber Security Act 2024*.

consumer has the meaning given by section 6.

defined support period has the meaning given by subclause 4(3) of Schedule 1.

Part 2—Security standards for smart devices

Division 1—Preliminary

5 Simplified outline of this Part

The rules may provide mandatory security standards for products that can directly or indirectly connect to the internet (called relevant connectable products) that will be acquired in Australia in specified circumstances.

Schedule 1 provides a security standard for consumer grade relevant connectable products (with some exceptions, see section 8) that will be acquired in Australia by a consumer.

Sections 15 and 16 of the Act require that:

(a) manufacturers must manufacture such products in compliance with the requirements of the security standard if they are aware, or could reasonably be expected to be aware, that the product will be acquired in Australia by a consumer; and

(b) those manufacturers must also comply with any other obligations relating to the product in the security standard (for example, obligations to publish information about the product); and

(c) if the product does not comply it must not be supplied in Australia if the supplier is aware, or could reasonably be expected to be aware, that the products will be acquired in Australia by a consumer; and

(d) those suppliers must supply the product in Australia accompanied by a statement of compliance which meets the requirements in the rules (see Division 3).

6 Meaning of consumer

A person has acquired particular goods as a ***consumer*** if the person would be taken to have acquired the goods as a consumer under section 3 of the Australian Consumer Law.

Division 2—Security standards for relevant connectable products

7 Purpose of this Division

For the purposes of subsection 14(1) of the Act, this Division provides security standards for specified classes of relevant connectable products that will be acquired in Australia in specified circumstances.

8 Security standards for consumer grade relevant connectable products

(1) Part 1 of Schedule 1 prescribes the security standard for the class of relevant connectable products that is all relevant connectable products that:

(a) are intended by the manufacturer to be used, or are of a kind likely to be used, for personal, domestic or household use or consumption; and

(b) are not any of the following products:

(i) a desktop computer or a laptop;

(ii) a tablet computer;

(iii) a smartphone;

(iv) therapeutic goods within the meaning of the *Therapeutic Goods Act 1989*;

(v) a road vehicle within the meaning of the *Road Vehicle Standards Act 2018*;

(vi) a road vehicle component within the meaning of the *Road Vehicle Standards Act 2018*.

(2) The specified circumstances are that the products will be acquired in Australia by a consumer.

Division 3—Statements of compliance

9 Requirements for statement of compliance

(1) For the purposes of subsection 16(5) of the Act, this section provides the requirements for a statement of compliance with the security standard in Part 1 of Schedule 1 (consumer grade relevant connectable products).

(2) The statement must be prepared by, or on behalf of, the manufacturer of the product.

(3) The statement must include the following information:

(a) the product type and batch identifier;

(b) the name and address of:

(i) the manufacturer of the product; and

(ii) an authorised representative of the manufacturer; and

(iii) each (if any) of the manufacturer's other authorised representatives that are in Australia;

(c) a declaration that the statement has been prepared by, or on behalf of, the manufacturer of the product;

(d) a declaration that, in the opinion of the manufacturer:

(i) the product has been manufactured in compliance with the requirements of the security standard; and

(ii) the manufacturer has complied with any other obligations relating to the product in the security standard;

(e) the defined support period for the product at the date the statement of compliance is issued;

(f) the signature, name and function of the signatory of the manufacturer;

(g) the place and date of issue of the statement of compliance.

10 Retention period for statement of compliance

For the purposes of subsections 16(2) and (4) of the Act, for statements of compliance with the security standard in Part 1 of Schedule 1 (consumer grade relevant connectable products) the period is 10 years.

Division 4—Notification of failure to comply with recall notice

11 Matters to be published with notification of failure to comply with recall notice

For the purposes of paragraph 20(e) of the Act, other matters that may be published are:

(a) details of the recall notice given to the entity under section 19 of the Act; and

(b) actions consumers are recommended to consider taking, for example:

(i) destroying the product; or

(ii) extra precautions to take when using the product.

Schedule 1—Security standards

Part 1—Security standard for consumer grade relevant connectable products

Note: See section 8

1 Definitions

In this Schedule:

application programming interface key means a string of characters used to identify and authenticate a particular user, product, or application so that it can access the application programming interface.

cryptographic key means data used to encrypt and decrypt data.

factory default state means the state of the product after factory reset or after final production or assembly.

good industry practice means the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced cryptographer engaged in the same type of activity.

hardware means a physical electronic information system, or parts thereof, capable of processing, storing or transmitting digital data.

incremental counter means a method of password generation in which multiple passwords are the same save for a small amount of characters which change per password to make them unique (such as ‘password1’ and ‘password2’).

keyed hashing algorithm means an algorithm that uses a data input and a secret key to produce a value which cannot be guessed or reproduced without knowledge of both the data input and the secret key.

manufacturer’s intended purpose of a product means the use for which the product is intended according to the data provided by the manufacturer, including on the label, in the instructions for use, or in promotional or sales materials or statements.

password does not include:

(a) a cryptographic key; or

(b) a personal identification number used for pairing in communication protocols which do not form part of the internet protocol suite; or

(c) an application programming interface key.

secret key means a cryptographic key intended to be known only by the person who encrypted or authorised the encrypting of the data, and any person authorised by the person.

security update has the meaning given by subclause 4(2).

unique per product means unique for each individual product of a given product class or type.

2 Passwords

(1) Passwords for use with a relevant connectable product in relation to any of the following must comply with the requirements in subclauses (2) and (3):
  (a) hardware of the product when the product is not in the factory default state;
  (b) software which is pre-installed on the product at the point at which the product is supplied to a consumer when the product is not in the factory default state;
  (c) software which is not pre-installed on the product at the point at which the product is supplied to a consumer and which must be installed on the product for all the manufacturer's intended purposes of the product that use:
    (i) hardware; or
    (ii) software that is pre-installed at the point at which the product is supplied to a consumer; or
    (iii) software that is installable.

(2) Passwords must be:
  (a) unique per product (subject to subclause (3)); or
  (b) defined by the user of the product.

(3) Passwords which are unique per product must not be:
  (a) based on incremental counters; or
  (b) based on or derived from publicly available information; or
  (c) based on or derived from unique product identifiers, such as serial numbers, unless this is done using an encryption method, or keyed hashing algorithm, that is accepted as part of good industry practice; or
  (d) otherwise guessable in a manner unacceptable as part of good industry practice.

3 Information on how to report security issues must be published

(1) The manufacturer of a relevant connectable product must publish the information in subsection (2) on how a person is to report security issues in relation to the product in respect of any of the following:
  (a) hardware of the product;
  (b) software which is pre-installed on the product at the point at which the product is supplied to a consumer;
  (c) software which must be installed on the product for all the manufacturer's intended purposes of the product that use:
    (i) hardware; or
    (ii) software that is pre-installed at the point at which the product is supplied to a consumer; or

(iii) software that is installable;

(d) software used for, or in connection with, any of the manufacturer's intended purposes of the product.

(2) The information that must be published is:

(a) at least one point of contact to allow a person to report the security issue to the manufacturer; and

(b) when a person who makes such a report will receive:

(i) an acknowledgement of the receipt of the report; and

(ii) status updates until the resolution of the reported security issues.

(3) The information published must be accessible, clear and transparent, and must be made available to a person:

(a) without prior request for such information being made; and

(b) in English; and

(c) free of charge; and

(d) without requesting the provision of personal information about the person.

4 Information on defined support period for security updates must be published

(1) The manufacturer of a relevant connectable product must publish the defined support period for security updates for the product in respect of the following:

(a) hardware of the product that is capable of receiving security updates;

(b) software that is capable of receiving security updates where that software is pre-installed on the product at the point at which the product is supplied to a consumer;

(c) software that is capable of receiving security updates which must be installed on the product for all the manufacturer's intended purposes of the product that use:

(i) hardware;

(ii) software that is pre-installed at the point at which the product is supplied to a consumer; or

(iii) software that is installable;

(d) software developed by or on behalf of any manufacturer that is capable of receiving security updates and used for, or in connection with, any of the manufacturer's intended purposes of the product.

(2) A ***security update*** is a software update that protects or enhances the security of the product, including a software update that addresses a security issue which has been discovered by or reported to the manufacturer.

(3) The ***defined support period*** is the period, expressed as a period of time with an end date, for which the security updates will be provided by, or on behalf of the manufacturer of the product.

(4) The manufacturer must not shorten the defined support period after it is published under subclause (1).

(5) If the manufacturer extends the defined support period, the new defined support period must be published by, or on behalf of, the manufacturer as soon as is practicable.

(6) The information published under subclause (1) or (5):
  (a) must be accessible, clear and transparent; and
  (b) must be made available to a person:
    (i) without prior request for such information being made; and
    (ii) in English; and
    (iii) free of charge; and
    (iv) without requesting the provision of personal information about the person; and
    (v) in such a way that is understandable by a reader without prior technical knowledge.

(7) If the manufacturer offers to supply the product on its website, or another website under its control, the manufacturer must ensure:
  (a) that the information required to be published under subclauses (1) and (5) is prominently published with the other information on the website that is intended to inform consumers' decisions to acquire the product; and
  (b) for each instance on the website that the main characteristics of the product are published, that the information required to be published under subclauses (1) and (5) is published alongside or otherwise given equal prominence to the publication of the main characteristics of the product.