Schedules

Schedule 1

Regulation 3

Security requirements for manufacturers

Passwords

1.—(1) The following sub-paragraphs apply to—

(a) hardware of the product when that 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 customer 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 customer and which must be installed on the product for all 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 customer; or

(iii) software that is installable.

(2) Passwords must be—

(a) unique per product; or

(b) defined by the user of the product.

(3) Passwords which are unique per product must not be—

(a) based on incremental counters;

(b) based on or derived from publicly available information;

(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;

(d) otherwise guessable in a manner unacceptable as part of good industry practice.

(4) In this paragraph, passwords do not include—

(a) cryptographic keys;

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

(c) application programming interface keys.

(5) In this paragraph—

"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;

"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 ("D") and a secret key ("K") to produce a value which cannot be guessed or reproduced without knowledge of both D and K;

"secret key" means a cryptographic key intended to be known only by the person ("P") who encrypted or authorised the encrypting of the data, and any person authorised by P;

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

Information on how to report security issues

2.—(1) The following sub-paragraphs apply to—

(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 customer;

(c) software which must be installed on the product for all 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 customer; or

(iii) software that is installable;

(d) software used for, or in connection with, any manufacturer's intended purpose of the product unless the product is a smartphone or a tablet computer capable of connecting to cellular networks.

(2) The following information must be published—

(a) at least one point of contact to allow a person ("P") to report to the manufacturer security issues relating to the categories listed in sub-paragraph (1) for any of the manufacturer's relevant connectable products for which they have an obligation under section 8 (duty to comply with security requirements); and

(b) when P will receive—

(i) an acknowledgment of the receipt of a security issues report; and

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

(3) The information in sub-paragraph (2) must be accessible, clear and transparent, and must be made available to P—

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

(b) in English;

(c) free of charge; and

(d) without requesting the provision of P's personal information.

Information on minimum security update periods

3.—(1) The following sub-paragraphs apply to—

(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 customer;

(c) software that is capable of receiving security updates which must be installed on the product for all 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 customer; 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 manufacturer's intended purpose of the product unless the product is a smartphone or a tablet computer capable of connecting to cellular networks.

(2) The defined support period must be published.

(3) If a manufacturer extends the minimum length of time for which security updates will be provided, creating a new defined support period, the new defined support must be published as soon as is practicable.

(4) The information in sub-paragraphs (2) and (3) must be accessible, clear and transparent, and must be made available to a person ("P")—

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

(b) in English;

(c) free of charge;

(d) without requesting the provision of P's personal information; and

(e) in such a way that is understandable by a reader without prior technical knowledge.

(5) Where a manufacturer publishes an invitation to purchase a relevant connectable product on its own website or on a non-paid for website under its control that contains information described in regulation 6(4)(a) of the 2008 Regulations, the information in sub-paragraphs (2) and (3) must be published alongside or otherwise given equal prominence to the information described in that regulation.

(6) The security requirements in this paragraph are not met if the defined support period is shortened after the publication of the information in sub-paragraph (2).

(7) In this paragraph—

"the 2008 Regulations" means the Consumer Protection from Unfair Trading Regulations 2008(**1**);

"invitation to purchase" has the meaning given in regulation 2(1) of the 2008 Regulations.

(**1**) S.I. 2008/1277.