ETSI TS/EN DDD DDD Vm.t.e (yyyy-mm)

Cyber Security for Consumer Internet of Things;

Requirements for [vertical domain]

<

**TECHNICAL SPECIFICATION/European Standard**

The present template proposes a structured way to extend ETSI TS 103 645 / ETSI EN 303 645 into a vertical domain, with adapted or new provisions in cyber security and data protection. It contains the methodology for the extension of ETSI EN 303 645, which can also be used for non-IoT devices such as the Home Gateway. It also embeds a placeholder for non-cyber provisions (e.g., for consumer IoT devices that are cyber-physical systems) in the form of an annex.

The current version of ETSI TS 103 645 / ETSI EN 303 645 is to be referenced.

Text in green (such as this note) is guidance text produced by TC CYBER and can be removed before publication. Text in black is normative text to be copied by editors into the vertical domain specification. It is recommended to keep boilerplate text as provided in the present template. Placeholder text such as [AAA] is to be filled in by editors on integrating the text into the vertical domain specification. Optional normative text, that can be copied by editors if applicable, is denoted with << >>.

The placeholder [vertical domain] is to be replaced by the name of the covered vertical domain throughout the document.

Each vertical domain is covered in one such document.

A vertical domain is first developed within a TS before being possibly turned into an EN.

A recording of a CYBER online session to explain the use of the template is available [here](https://docbox.etsi.org/CYBER/CYBER/30-Inbox/Vertical%20IoT%20template%20use%20tutorial%20720p.mov). Note that it is not a formal training.

Reference

<Workitem>

Keywords

<keywords>

***ETSI***

650 Route des Lucioles

F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B

Association à but non lucratif enregistrée à la

Sous-Préfecture de Grasse (06) N° w061004871

***Important notice***

The present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at [www.etsi.org/deliver](http://www.etsi.org/deliver).

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at <https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

***Notice of disclaimer & limitation of liability***

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or

other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI yyyy.

All rights reserved.

Contents

Intellectual Property Rights 5

Foreword 5

Modal verbs terminology 6

Executive summary 6

Introduction 6

1 Scope 7

2 References 7

2.1 Normative references 7

2.2 Informative references 7

3 Definition of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Methodology and general requirements 8

4.1 Introduction 8

4.2 Handling of provisions 8

4.3 Naming conventions 9

4.4 Reporting implementation 11

4.5 [Further vertical domain specific clauses] 11

5 Adapted cyber security provisions for [vertical domain] 11

5.1 No universal default passwords 11

5.2 Implement a means to manage reports of vulnerabilities 11

5.3 Keep software updated 11

5.4 Securely store sensitive security parameters 11

5.5 Communicate securely 11

5.6 Minimize exposed attack surfaces 11

5.7 Ensure software integrity 11

5.8 Ensure that personal data is secure 11

5.9 Make systems resilient to outages 12

5.10 Examine system telemetry data 12

5.11 Make it easy for users to delete user data 12

5.12 Make installation and maintenance of devices easy 12

5.13 Validate input data 12

6 Adapted data protection provisions for [vertical domain] 12

7 Additional cyber security provisions for [vertical domain] 12

7.1 New topic #1 12

7.2 New topic #2 12

8 Additional data protection provisions for [vertical domain] 13

8.1 New topic #1 13

8.2 New topic #2 13

Annex A (informative): Basic concepts, threat models, risk analysis 13

Annex B (informative): Implementation conformance statement pro forma 14

Pro forma copyright release text block 14

<L.N> The right to copy 14

Annex C (informative): Non-cyber security aspects for [vertical domain] 15

Annex D (normative or informative): [Further vertical domain specific annexes] 16

History 17

# Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

# Foreword

EITHER

<< This Technical Specification (TS) has been produced by ETSI Technical Committee {ETSI Technical Committee|ETSI Project|<other>} <long techbody> (<short techbody>). >>

For TC CYBER this can be: "This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER)."

OR

<< This European Standard (EN) has been produced by {ETSI Technical Committee|ETSI Project|<other>} <long techbody> (<short techbody>){|, and is now submitted for the {combined Public Enquiry and Vote|Vote phase of the ETSI standards {Membership Approval Procedure||<approval phase> phase of the ETSI standards EN Approval Procedure|Two-step Approval Procedure}}}. >>

For TC CYBER this can be: "This draft European Standard (EN) has been produced by ETSI Technical Committee Access, Terminals, Transmission and Multiplexing (ATTM), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure."

|  |
| --- |
| **Proposed national transposition dates** |
| Date of latest announcement of this EN (doa): | 3 months after ETSI publication |
| Date of latest publication of new National Standardor endorsement of this EN (dop/e): | 6 months after doa |
| Date of withdrawal of any conflicting National Standard (dow): | 6 months after doa |

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Executive summary

To keep with the approach taken in ETSI EN 303 645 / ETSI TS 103 645, no executive summary is provided, and this clause can be removed.

# Introduction

The introduction clause can refer and extend that of ETSI TS 103 645 / ETSI EN 303 645 according to the vertical domain of the present document.

Explain how this vertical standard builds on ETSI EN 303 645 / ETSI TS 103 645 and how it fits into the broader consumer IoT document set. This clause is to indicate whether a baseline level of security is considered (as with ETSI TS 103 645 / ETSI EN 303 645) or if some provisions are meant to cover higher levels of security. In the latter, a mapping of the provisions to the security level can be provided in an ad-hoc annex and referenced here.

# 1 Scope

The present document specifies …

The scope clause can refer and extend that of ETSI TS 103 645 / ETSI EN 303 645 according to the vertical domain of the present document. It should remind that the key domain is the consumer IoT domain, and it should make clear that the present document extends the normative work of ETSI TS 103 645 / ETSI EN 303 645. Moreover, the scope is intended to explain the necessity of a TS / EN covering the vertical domain, for example by naming the differences to a "generic" consumer IoT device. It is reminded that the scope clause is usually aligned with the NWI description.

# 2 References

## 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 103 645 Vn.n.n … or ETSI EN 303 645 Vn.n.n

A normative reference to ETSI TS 103 645 or ETSI EN 303 645 with an appropriate version is to be the first normative reference. It is to be ensured that the referenced version number of the ETSI TS 103 645 or ETSI EN 303 645 is up to date. If ETSI EN 303 645 is referenced, ETSI TS 103 645 will have to be replaced by the EN in the content of the deliverable.

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1]

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

This clause is to import definitions from clause 3.1 of normative reference [1] and to provide additional definitions below. It is recommended to carefully consider the definitions provided by [1] and to give them preference, when possible, to minimise overlapping of terms and maximise reusability across verticals.

For the purposes of the present document, the [following] terms [given in ... and the following] apply:

Term format**<term>:** <definition of term>

## 3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

Symbol format<symbol> <Definition of symbol>

## 3.3 Abbreviations

This clause is to import definitions from clause 3.3 of normative reference [1] if these are applicable and to provide additional definitions below. It is recommended to carefully consider the abbreviations provided by [1] and to ensure that there is no overlapping of abbreviations with different meanings.

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

<ABBREVIATION> <Definition of abbreviation>

# 4 Methodology and general requirements

## 4.1 Introduction

Here a short introduction on the approach taken to extend ETSI TS 103 645 can be given. Starting with clause 4.5 methodology aspects that are specific to the vertical domain can be specified.

## 4.2 Handling of provisions

The present document adopts the provisions of ETSI TS 103 645 [1] / ETSI EN 303 645 [1] as a baseline for the [vertical domain]. The methodology used for the adoption is described in the present clause, which includes different operations to modify provisions from ETSI TS 103 645 [1] / ETSI EN 303 645 [1] and add new provisions specific to the [vertical domain].

**All provisions from ETSI TS 103 645 [1] / ETSI EN 303 645 [1] shall apply in the present document, unchanged, to the consumer IoT device in the [vertical domain], unless otherwise noted in the present document.**

In case constrained devices are not in scope of the vertical domain, the following two sentences are to be added. If not, they are to be removed.

<< Consumer IoT devices in the [vertical domain] are not constrained devices. Consequently, all provisions from ETSI TS 103 645 [1] regarding constrained devices are adjusted accordingly. >>

Some provisions in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] address constrained devices using conditions or take into account other conditions. Generally, provisions can be adjusted depending on the applicability of these conditions in the vertical domain as follows:

| **Status in ETSITS 103 645 [1]** | **Option for new status in vertical domain** |
| --- | --- |
| M C | M |
| R | M |
| R C | R |
| R C | M C |
| R C | M |
| M - Mandatory requirementR - RecommendationM C - Mandatory requirement and ConditionalR C - Recommendation and Conditional |

There are different types of modifications indicated by a naming convention as described in clause 4.3. Within clauses 5 and 6 of the present document, the following modifications can be applied to the set of provisions defined in ETSI TS 103 645 [1] / ETSI EN 303 645 [1]:

Modified provisions are meant to further clarify an existing provision from TS 103 645 and are not to be used to expand its scope. For such purpose, new provisions are to be used.

**Information**: Providing additional information (in the form of informative text) to an unmodified provision. The original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] is still valid.

**Promotion**: Promoting a recommendation to a mandatory provision. The wording of the provision remains as in the original provision, but the promoted modal verb is replaced by the new modal verb (e.g. "should" is replaced by "shall"). The original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] is replaced by the promotion and is not valid anymore.

**Refinement**: Refining a provision with additions or modifications to its normative definition text, including stronger scoping of conditionality. The original scope and spirit remain in force. The original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] is replaced by the refinement and is not valid anymore.

NOTE: A refinement can be used to scope the conditionality of a provision, i.e. to remove one or more conditions from the provision, as part of the clarification on the provision's constraints.

**Extension**: Extending an existing provision with one or more new sub-provisions. The original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] is still valid.

**Substitution**: Replacing a recommendation that is not applicable for the [vertical domain] with another recommendation of equivalent effect (that provides, possibly in combination with other recommendations or provisions, the same security outcome as the replaced recommendation). The original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] is replaced by the substitution and is not valid anymore.

**Exclusion** (only possible for recommendations and conditional provisions): Declaring a recommendation or conditional provision as "not applicable" for the [vertical domain]. The original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] is excluded and is not valid anymore.

NOTE: Mandatory provisions of the EN cannot be made non-applicable in a vertical standard. A device that conforms to a vertical standard also conforms to ETSI TS 103 645 [1] / ETSI EN 303 645 [1].

The present document allows to define new provisions within the clauses 7 and 8 that are not covered in ETSI TS 103 645 [1] / ETSI EN 303 645 [1]. There is one type of new provisions, that is also covered by the naming convention in clause 4.3:

The clauses for new provisions are structured following the structure of ETSI TS 103 645 [1] / ETSI EN 303 645 [1]. Therefore clause 7 contains new "Cyber security provisions" of the vertical domain and clause 8 contains new "Data protection provisions" for the vertical domain. Sub-clauses can also be used in both clauses to group related provisions.

**Addition**: Defining a new provision specific to the [vertical domain] that cannot be linked to any provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1].

## 4.3 Naming conventions

The provisions in the present document are named following the naming conventions described in the present clause.

It is recommended that, as with ETSI TS 103 645 [1], the modal verbs 'shall' and 'should' in clauses 5 to 8 are only used within the normative text of the provisions, and the provisions themselves, when defined, are named in **bold characters**.

To denote unmodified provisions, the original provision reference from ETSI TS 103 645 [1] / EN 303 645 [1] is used. Unmodified provisions are not copied from ETSI TS 103 645 [1] / ETSI EN 303 645 [1] into the present document. However, they can be referenced if additional information is available for the provision in the context of the [vertical domain].

EXAMPLE 1: In the context of provision 5.1-1of ETSI TS 103 645 [1] / EN 303 645 [1], the following information is provided.

Each provision contains an acronym representing the [vertical domain]. The acronym for the [vertical domain] is set to [AAA].

EXAMPLE 2: Exemplary acronyms are "SDL" for Smart Door Locks or "HG" for Home Gateways, and so forth.

Names for provisions that are specific to the present document are constructed as follows:

The name starts with the string "Provision" to which the acronym "[AAA]" is appended.

A provision identifier (id) is appended. An example id is 5.1-1.

One or more suffixes are appended (according to the types of provisions as described in clause 4.2).

NOTE: A provision can be at the same time promoted and refined, in which case the two suffixes are appended to its name.

For provisions that are extensions, an alphabetical index is appended, that is unique to the provision, for example, "-a". The alphabetical index is appended only in cases where there is more than one extension to a given provision.

The following list describes the suffixes depending on the type of the provision as described in clause 4.2:

**Information**: The id is the id of the original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] additional informative information is provided for. The suffix is "(information)".

EXAMPLE 3: **Provision [AAA] 5.8-3 (information)** In the context of the [vertical domain], typical external sensing capabilities are cameras and microphones.

NOTE: The provided text in example 3 could be also given as a note as follows:
“**Provision [AAA] 5.8-3 (information)** NOTE: In the context of the [vertical domain], typical external sensing capabilities are cameras and microphones.”
Instead of writing NOTE before the informative text, one could also write EXAMPLE in the beginning of the informative text, if applicable.

**Promotion**: The id is the id of the original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] that is promoted. The suffix is "(promoted)".

EXAMPLE 4: **Provision [AAA] 5.2-2 (promoted)** Disclosed vulnerabilities shall be acted on in a timely manner.

**Refinement**: The id is the id of the original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] that is refined. The suffix is "(refined)".

EXAMPLE 5: **Provision [AAA] 5.2-2 (refined)** Disclosed vulnerabilities should be acted on in a timely manner, with a maximum of 90 days after reporting to the manufacturer.

EXAMPLE 6: **Provision [AAA] 5.2-2 (promoted) (refined)** Disclosed vulnerabilities shall be acted on in a timely manner, with a maximum of 90 days after reporting to the manufacturer.

**Extension**: The id is the id of the original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] that is extended. The suffix is "(extended)".

EXAMPLE 7: **Provision [AAA] 5.3-1 (extended)-a** For each software component that is not updateable, a justification for the absence of software updates shall be provided.

EXAMPLE 8: **Provision [AAA] 5.3-1 (extended)-b** For each software component that is not updateable, this fact should be indicated in the user manual.

**Substitution**: The id is the id of the original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] that is substituted. The suffix is "(substituted)".

EXAMPLE 9: **Provision [AAA] 5.3-12 (substituted)** The user should be notified within the update notification whether the application of a software update will disrupt the basic functioning of the device.

**Exclusion**: The id is the id of the original provision in ETSI TS 103 645 [1] / ETSI EN 303 645 [1] that is excluded. The suffix is "(excluded)".

EXAMPLE 10: **Provision [AAA] 5.3-14 (excluded)** The provision is not applicable for the [vertical domain] and shall not apply.

**Addition**: The id is a new and unique id added in clause 7 or 8 that reflects the clause in which it is defined. The suffix is "(added)".

EXAMPLE 11: **Provision [AAA] 7.1-1 (added)** User data on the device should be backed up periodically.

## 4.4 Reporting implementation

Provision 4-1 in TS 103 645 [1] / ETSI EN 303 645 [1] addresses provisions in the ETSI TS 103 645 [1] / ETSI EN 303 645 [1] only. It can be extended to cover the provisions from the present document as well by using an extension described in clause 4.2.

<< **Provision [AAA] 4-1 (extended)** A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the device. >>

## 4.5 [Further vertical domain specific clauses]

Starting with (optional) clause 4.5 and beyond, methodology aspects that are specific to the vertical domain can be provided, as required.

# 5 Adapted cyber security provisions for [vertical domain]

## 5.1 No universal default passwords

Two options are possible:

<< Existing provisions from ETSI TS 103 645 [1] / ETSI EN 303 645 [1] clause 5.1 are modified as follows. >>

or

<< No modifications to the provisions from ETSI TS 103 645 [1] / ETSI EN 303 645 [1] clause 5.1 are defined in the present document. >>

If provisions from ETSI TS 103 645 / ETSI EN 303 645 are modified in each clause 5.x, these are listed in the order they appear in ETSI TS 103 645 / ETSI EN 303 645. This way, the reader can quickly skim through the clause, even if there are gaps. If a provision is modified, it appears in the clause according to the rules defined in clauses 4.2 and 4.3.

## 5.2 Implement a means to manage reports of vulnerabilities

Refer to normative and guidance text provided in clause 5.1.

## 5.3 Keep software updated

Refer to normative and guidance text provided in clause 5.1.

## 5.4 Securely store sensitive security parameters

Refer to normative and guidance text provided in clause 5.1.

## 5.5 Communicate securely

Refer to normative and guidance text provided in clause 5.1.

## 5.6 Minimize exposed attack surfaces

Refer to normative and guidance text provided in clause 5.1.

## 5.7 Ensure software integrity

Refer to normative and guidance text provided in clause 5.1.

## 5.8 Ensure that personal data is secure

Refer to normative and guidance text provided in clause 5.1.

## 5.9 Make systems resilient to outages

Refer to normative and guidance text provided in clause 5.1.

## 5.10 Examine system telemetry data

Refer to normative and guidance text provided in clause 5.1.

## 5.11 Make it easy for users to delete user data

Refer to normative and guidance text provided in clause 5.1.

## 5.12 Make installation and maintenance of devices easy

Refer to normative and guidance text provided in clause 5.1.

## 5.13 Validate input data

Refer to normative and guidance text provided in clause 5.1.

No further clauses are to be defined after clause 5.13, unless it is defined in ETSI TS 103 645 / ETSI EN 303 645. This avoids potential incompatibilities between future versions of the present document and ETSI TS 103 645 / ETSI EN 303 645.

# 6 Adapted data protection provisions for [vertical domain]

Two options are possible:

<< Existing provisions from ETSI TS 103 645 [1] / ETSI EN 303 645 [1] clause 6 are modified as follows. >>

or

<< No modifications to the provisions from ETSI TS 103 645 [1] / ETSI EN 303 645 [1] clause 6 are defined in the present document. >>

Refer to normative and guidance text provided in clause 5.1.

# 7 Additional cyber security provisions for [vertical domain]

In case the vertical domain does not require new provisions, clause 7 can be left "void" to keep the structure of the document in line with the template and allow new provisions to be added in revisions of the present document.

## 7.1 New topic #1

New provisions can be added according to the rules defined in clauses 4.2 and 4.3.

## 7.2 New topic #2

…

# 8 Additional data protection provisions for [vertical domain]

In case the vertical domain does not require new provisions, clause 8 can be left "void" to keep the structure of the document in line with the template and allow new provisions to be added in revisions of the present document.

## 8.1 New topic #1

New provisions can be added according to the rules defined in clauses 4.2 and 4.3.

## 8.2 New topic #2

…

Annex A (informative):
Basic concepts, threat models, risk analysis

In a similar fashion as with ETSI TS 103 645 / ETSI EN 303 645 Annex A, the present annex can provide details of the architecture of a consumer IoT deployment in the considered vertical domain and the related device states.

The annex is also meant to address:

* threat model,
* risk analysis, and
* other considerations that can provide background information to the refinement of provisions, promotion of recommendations into mandatory provisions, and the introduction of new provisions in the present document.

This information can be provided within the annex or via reference to other deliverable(s) containing the information.

Annex B (informative):
Implementation conformance statement pro forma

# Pro forma copyright release text block

This text box shall immediately follow after the heading of an element (i.e. clause or annex) containing a pro forma or template which is intended to be copied by the user. Such an element shall always start on a new page.

# <L.N> The right to copy

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the <pro formatype> pro forma in this {clause|annex} so that it can be used for its intended purposes and may further publish the completed <pro formatype>.

Serves the same purpose as ETSI TS 103 645 / ETSI EN 303 645 Annex B.

The introductory text and ICS pro forma are to be aligned with the "[Principles for drafting ETSI deliverables with the use of skeletons](https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/Principles_for_drafting_ETSI_deliverables.docx)" that are valid at the time of developing the present document, taking into account the use of the ICS in ETSI TS 103 701.

All provisions from the present document are to be listed in the ICS pro forma table. In addition, all provisions from ETSI TS 103 645 [1] / ETSI EN 303 645 [1] that have not been promoted and/or refined or substituted or excluded in the present document shall be listed in the ICS pro forma table.

An ICS pro forma table with some exemplary entries is shown as follows. To show different examples and since clause 5.1 has no recommendation provisions, some provisions are skipped in this exemplary table, denoted by "**...**". However, in the vertical document no provision is to be skipped in the ICS pro forma table.

|  |
| --- |
| **Clause number and title** |
| **Reference** | **Status** | **Support** | **Detail** |
| **5.1 No universal default passwords** |
| Provision [AAA] 5.1-1 (refined) | M |  |  |
| **…** | **…** |  |  |
| **5.2 Implement a means to manage reports of vulnerabilities** |
| Provision 5.2-1 | M |  |  |
| Provision [AAA] 5.2-2 (promoted) | M |  |  |
| Provision [AAA] 5.2-3 (excluded) | R |  |  |
| **5.3 Keep software updated** |
| Provision [AAA] 5.3-1 (substituted) | R |  |  |
| **…** | **…** |  |  |

Annex C (informative):
Non-cyber security aspects for [vertical domain]

This annex is a placeholder to provide an informative overview of the wider security challenges for consumer IoT devices / systems for the vertical domain, such as those that characterise them as a cyber-physical system. Topics can cover electromechanical security, mechanical security, perimeter security, and so forth. References to relevant specifications covering these topics can be given.

The fulfilment of this annex is optional. In case no such information will be provided, insert the sentence "There is no specific information for the [vertical domain]".

Annex D (normative or informative):
[Further vertical domain specific annexes]

Starting with (optional) annex D and beyond, further vertical domain specific aspects can be provided, as required.

# History

|  |
| --- |
| **Document history** |
| <Version> | <Date> | <Milestone> |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |