 <b>CYCLONE</b> PHARMACEUTICALS	<b>Security Risk Management Plan of Paperless GMP Software</b>	PROTOCOL NO.
		EFFECTIVE DATE :
		PAGE NO.:

# Security Risk Management Plan of Paperless GMP software

TITLE	
AUTHORING GROUP	
DATE	
SUPERSEDE PROTOCOL NO. :	

### TABLE OF CONTENTS

Sr. No.		Page No.
<b>1</b>	<b>Introduction</b>	
	1.1 Document overview	
	1.2 References	
	1.2.1 Project Reference	
	1.2.2 Standard and regulatory references	
	1.2.3 Definitions	
	1.2.4 Conventions	
<b>2</b>	<b>Responsibilities</b>	
<b>3</b>	<b>Risk management process</b>	
	3.1 Context establishment	
	3.2 Risk assesment	
	3.2.1 Identification	
	3.2.2 Analysis	
	3.2.3 Evaluation	
	3.3 Risk treatment	
	3.4 Risk acceptance	
	3.5 Risk communication	
	3.6 Post-production monitoring and review	
<b>4</b>	<b>Ranking system for Security risk analysis</b>	
	4.1 Probability of occurrence	
	4.2 Severity	
	4.3 Other criteria	
	4.4 Risk priority number	
<b>5</b>	<b>Relationships with other risk management processes</b>	
	5.1 Ranking system of safety risks when security breach is the harzardous phenomenon	
	5.2 Communication with safety risk management team	
	5.3 Communication with usability engineering team	

	<b>Security Risk Management Plan of Paperless GMP Software</b>	PROTOCOL NO.
		EFFECTIVE DATE :
		PAGE NO.:

## 1 Introduction

### 1.1 Document overview

Describe the purpose of the document

This document contains the security risk management plan for Paperless GMP Software. It covers the management all security-related risks during the lifecycle of the device, in design and development, and in maintenance. It also contains the provisions about relationships with the ISO 14971 safety risk management process, and IEC 62366-1 usability engineering process.

### 1.2 References

#### 1.2.1 Project References

#	Document Identifier	Document Title
[R1]	ID	Add your documents references. One line per document

#### 1.2.2 Standard and regulatory References

#	Document Identifier	Document Title
[STD1]		Add your documents references. One line per document

#### 1.2.3 Definitions

**Information security risk:** potential that a given threat will exploit vulnerabilities of an asset or group of assets, and thereby cause harm to the organization.

You may add here other definitions like Asset, Threat, Vulnerability found in IEC 81001-5-1.

#### 1.2.4 Conventions

**Security risk and Cybersecurity risk** are used indifferently in this document as synonyms of **Information security risk** according to the definition above.

## 2 Responsibilities

Describe the organization of the team responsible for risk management. You may add an organization chart or add a reference to your project management plan, where the organization of the project should be already described.

Either describe the responsibilities in plain text:

The security risk manager is in charge of the security risk. The Quality and regulatory manager is in charge of the relationships with the ISO 14971 safety risk management process.

Or use a table :

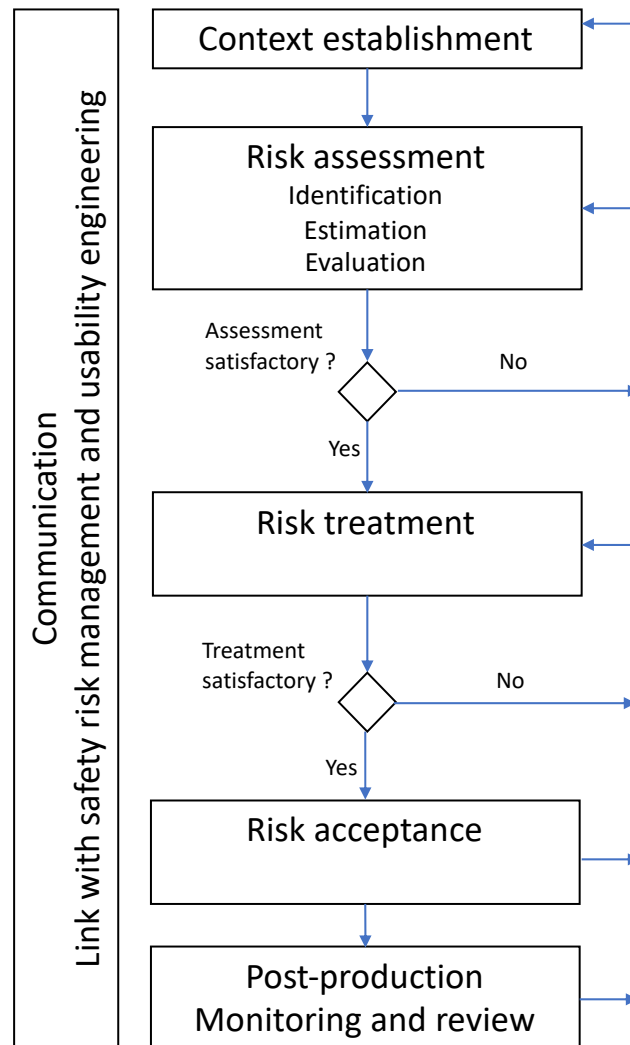
Person	Responsibility
Security Officer	<ul style="list-style-type: none"> <li>Overall risk management process responsibility</li> </ul>
Project Manager	<ul style="list-style-type: none"> <li>Risk management process responsibility during design</li> </ul>
Hardware design manager	<ul style="list-style-type: none"> <li>Hardware security risks</li> </ul>
System design manager	<ul style="list-style-type: none"> <li>System / network security risks</li> </ul>
Software design manager	<ul style="list-style-type: none"> <li>Software security risks</li> </ul>
Quality Manager	<ul style="list-style-type: none"> <li>Independent review of Risk Management File</li> </ul>
Quality Manager	<ul style="list-style-type: none"> <li>Interface with the safety risk management process</li> </ul>
Deployment Manager	<ul style="list-style-type: none"> <li>Interface with IT services in healthcare center</li> </ul>
Customer Service Manager	<ul style="list-style-type: none"> <li>Interface with end-users in healthcare center</li> </ul>

You may also explain here how adverse events are escalated in the organization. Eg : Adverse events or risk of adverse events detected throughout the organization shall be immediately reported to the security officer.

### 3 Risk management process

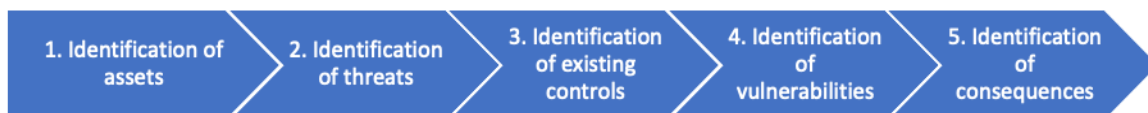
The process described below is inspired from the risk management process presented in ISO 27005 (which stems from risk management process presented in ISO 31000), with arrangements for compliance to IEC 81001-5-1 and ISO 14971.

The risk management process is an iterative process allowing to increase the depth and details of risk assessment at each iteration.



### 3.1 Context establishment and threat modelling


These two steps (1 & 2 below) allow to identify assets and threats.



Establishing the context consists in defining the scope and boundaries, and describing the following items, as appropriate:

- The Medical Device (hardware, software, network...)
- Its Accessories,
- Its Environment
  - Operating Room
  - Patient Room
  - At Home

- Other Connected Devices,
  - Medical devices,
  - Non-medical devices,
  - Cloud servers
- The processes involved in the lifecycle of the device:
  - Internal processes,
  - Outsourced processes and
  - Client/user processes,
- The users and user profiles
  - Client users,
  - Users of the manufacturer (e.g. customer support)
- The level of education of users,
- The use cases associated to the users and user profiles,
- The types of data handled in the device
  - Medical and personal data,
  - Data from sensors,
  - Configuration data,
  - Logs
- The hardware network interfaces
  - Bluetooth,
  - Wi-Fi, Zigbee,
  - RJ45,
- The software network interfaces and protocols
  - HTTP, TCP, UDP,
  - SOAP, REST
  - Network Ports
- The data input/output streams
  - With connected devices,
  - Through removable media,
  - Internally between sub-systems of the device,
- The COST/SOUP used in software
  - Maintained software
  - Supported software (see IEC 81001-5-1)
- The constraints affecting the device
  - On the device,
  - On manufacturer processes,
  - On user processes, E.g. end-users generally don't accept to un-scrub and scrub for IT security reasons,
  - Regulatory requirements: GDPR, HIPAA...
- Constraints regarding emergency access to the device for patient safety, bypassing security measures.

	<b>Security Risk Management Plan of Paperless GMP Software</b>	PROTOCOL NO.
		EFFECTIVE DATE :
		PAGE NO.:

All items listed above in 2<sup>nd</sup> level bullets are practical examples, other cases may be applicable to the device.

### Assets

An asset is anything of value for the manufacturer or for the end-user.

Assets can be:

- Hardware,
- Software,
- Data,
- Other tangible or intangible assets.

Examples:

- The medical device itself,
- Its accessories,
- Devices connected to the medical device,
- Cloud servers,
- Patient data,
- Diagnosis or Treatment data,
- Other data.

Knowing the assets contributes to identify the magnitude of the consequences of adverse event. Eg: the consequences won't have the same order of magnitude if the device is a simple object, a cloud server.

### Threats


A threat is anything (human, phenomenon, accidental, deliberate) susceptible to result in a damage on one or more assets.

Examples:

- Script kiddies
- Academic researchers
- Criminal organizations
- Inexperienced users
- Natural events

This context allows to identify the threats, documented in the threat modelling. The context and threat modelling can be described in data flow diagrams (DFD), use cases, hardware architecture, system architecture, software architecture, as appropriate.

Some information may already be documented in the usability engineering file and shall be referenced by the threat modelling documentation. E.g. Users, user profiles, use cases.

	<b>Security Risk Management Plan of Paperless GMP Software</b>	PROTOCOL NO.
		EFFECTIVE DATE :
		PAGE NO.:

The constraint of emergency access to the device, bypassing security measures, shall be described in the context.

Additionally, the manufacturer shall provide justification for any exclusion from the scope.

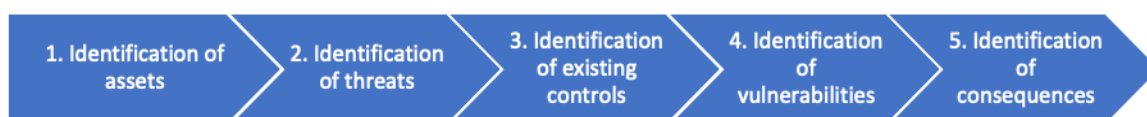
### 3.2 Risk assessment

Based on the threat model documented in the previous step, the risks shall be identified, analysed and evaluated according to the objectives of the risk management process and the ranking system for security risk analysis.

A preliminary risk assessment, together with the threat modelling, may be documented at the beginning of the design project, or before design (e.g. in feasibility / mock-up etc.) and reviewed in the design input data.

#### 3.2.1 Identification

(Steps 3, 4 and 5 below)



#### Existing controls.

Existing or planned controls should be identified. They can be identified inside the manufacturer's organization or in the target environments or other environments (healthcare provider, datacenter service supplier...).

Existing or planned controls should be assessed to determine if they are effective, sufficient and justified.

#### Vulnerabilities

Vulnerabilities shall be identified. Vulnerabilities may come from design decisions, misuse of the device, software SOUPs, organizations, processes, etc.

Vulnerabilities can be found in catalogs like the Common Vulnerabilities and Exposures List, the National Health ISAC and release notes of SOUP /COTS editors.


#### Consequences

The consequences that loss of confidentiality, integrity and availability may have on the assets shall be identified. The consequences on patient safety shall also be identified.

#### Records

Assets, threats, vulnerabilities, existing controls and consequences shall be recorded in the security risk assessment report.



	<b>Security Risk Management Plan of Paperless GMP Software</b>	PROTOCOL NO.
		EFFECTIVE DATE :
		PAGE NO.:

### 3.2.2 Analysis

The risk analysis is performed with the use of the ranking system described in section 4 of this document, and with the data collected in the previous steps:

- The identification of the consequences on assets allow to determine the impact magnitude of the risk,
- The identification of threats, vulnerabilities, and incident scenarios allow to determine the likelihood of a risk.

#### Records

For each incident scenario: probability of occurrence, severity, other criteria, and RPN are recorded in the risk assessment report.

### 3.2.3 Evaluation

The RPN are compared against risk acceptance criteria described in section 4. Legal and regulatory requirements shall be included in the evaluation of the acceptance of risks.

#### Records

For each incident scenario: risk acceptance, and decision.

### 3.3 Risk treatment

The term “risk treatment” is used in ISO 27005. Note that the meaning of “risk treatment” is broader than “risk control” or “risk mitigation” commonly used in medical device industry.

For information, risk treatment options are:

- Risk modification or risk control,
- Risk retention (retaining the risk without further action),
- Risk avoidance (avoiding the conditions giving rise to the risk),
- Risk sharing (sharing the risk with another party. E.g. insurance company).

Note that risk retention and sharing shall be acceptable from a safety (ISO 14971) point of view. These to kind of actions won't be possible for security risks with a safety impact.

Risk controls shall be sought in this order of precedence:

- Security by design,
- Security measures implemented in production or servicing,
- Information for security.

Risk control should be carried out to decrease the RPN of the residual risk As Low As Reasonably Possible (ALARP), with economic considerations. If the risk has an impact on patient safety, the risk treatment (risk control) shall be carried out with acceptance criteria related to patient safety.

	<b>Security Risk Management Plan of Paperless GMP Software</b>	PROTOCOL NO.
		EFFECTIVE DATE :
		PAGE NO.:

The security vulnerabilities or impacts on patient safety arising from risk treatment shall also be assessed.

#### Records

For each incident scenario: the risk treatment plan.

### **3.4 Risk acceptance**

The reevaluation of the risk is performed with the use of the ranking system described in section 4 of this document, and with the risk treatment plan.

A security risk may be deemed accepted even if it doesn't match the risk acceptance criteria of section 4, with justification to override the acceptance criteria.

#### Records

For each incident scenario: the risk acceptance and justification as appropriate.

### **3.5 Risk communication**

The risk assessment report is communicated internally to the design team. The risk assessment report shall be an agenda item of design reviews, and validation reviews.

Parts of the risk assessment report may also be communicated externally to service providers or suppliers, as appropriate. When a supplier requires knowledge of the risk assessment report, it should be determined if this supplier shall be placed in the list of critical suppliers.

### **3.6 Post-production monitoring and review**

The Risk Management File is systematically reviewed and updated, especially when:

- The product is modified,
- The context changes,
- Assets, threats, vulnerabilities change,
- Analysis of data of post marketing surveillance triggers a reevaluation (internal defects, customer requests, maintenance, vigilance bulletins, security incidents, field information from any source).

The review of post-marketing data is performed **quarterly / annually / other period**. Reviews and updates to any risk will be documented, approved, and included within the Risk Management File.

The review includes an evaluation of the relevance of the ranking system and the need to update it upon business or regulatory context.

#### 4 POSSIBILITY 1: Ranking system for security risk analysis based on CVSS

According to UL 2900-1, the risk criteria shall be based on CVSS or derived from CVSS. When claiming compliance to UL 2900, a possibility is to use the probability based on CVSS:

P = CVSS base score [0 ; 10]

Ranking	Definition	Comment
Critical	$9 \leq \text{CVSS base score} \leq 10$	Risk is unacceptable
High	$7 \leq \text{CVSS base score} < 9$	Risk is unacceptable
Medium	$4 \leq \text{CVSS base score} < 7$	Risk is tolerable
Low	$0 < \text{CVSS base score} < 4$	Risk is acceptable
None	$0 = \text{CVSS base score}$	No risk

Remark, it may be possible to tailor the acceptability to the SL-C of the software:

Ranking	Definition	SL-C 1	SL-C 3
Critical	$9 \leq \text{CVSS base score} \leq 10$	Risk is unacceptable	Risk is unacceptable
High	$7 \leq \text{CVSS base score} < 9$	Risk is tolerable	Risk is unacceptable
Medium	$4 \leq \text{CVSS base score} < 7$	Risk is acceptable	Risk is tolerable
Low	$0 < \text{CVSS base score} < 4$	Risk is acceptable	Risk is acceptable
None	$0 = \text{CVSS base score}$	No risk	No risk

#### 5 POSSIBILITY 2 Ranking system for security risk analysis

This second possibility may be more convenient for medical device manufacturer teams, as it is closer to what they know with safety risk management.

This section describes how the risk priority number is deduced from the characteristics of the risk:


- Probability of occurrence,
- Severity of consequences
- Other criteria (if any).

Describe in sub sections how you quantify your criteria, like these:

##### 5.1 Probability of occurrence

You can use quantitative or qualitative criteria. Here is an example.

Ranking	Definition	Probability (P)
5	Often occurs, once a week	Frequent (very high probability)
4	Could easily happen, once a month	Probable (high probability)
3	Could happen or known to happen, once a year	Occasional (moderate probability)
2	Hasn't happened yet but could,	Unlikely (low probability)

	<b>Security Risk Management Plan of Paperless GMP Software</b>	PROTOCOL NO.
		EFFECTIVE DATE :
		PAGE NO.:

Ranking	Definition	Probability (P)
	once in device lifetime	
1	Conceivable but only in extreme circumstances, less than once in device lifetime	Very Unlikely (very low probability)

## 5.2 Severity

Use quantitative or qualitative criteria. Here is an example. You may add explicit links with consequences on HIPAA or GDPR compliance.

Ranking	Definition	Severity
5	Significant loss of confidentiality or data integrity. Threatens financial health of manufacturer.	Catastrophic
4	Some loss of confidentiality or data integrity. Some consequences on financial health of manufacturer.	Critical
3	Small, isolated loss of confidentiality or data integrity. Small consequences on financial health of manufacturer.	Moderate
2	Isolated, limited leak of non-sensitive data. May incur costs to recover leaked data.	Minor
1	Recoverable data loss, Non-sensitive data leak. Negligible cost.	Negligible

## 5.3 Other criteria

Add other criteria, or remove this section

## 5.4 Risk Priority Number

A rule of your choice, like.

$$\text{Risk priority number} = \begin{matrix} \text{criterion 1} \\ \times \text{criterion 2} \\ \dots \\ \times \text{criterion n} \end{matrix}$$

Example of cross-table of RPN with two criteria:

CROSS TABLE OF RISK PRIORITY NUMBER					
	Negligible 1	Minor 2	Moderate 3	Critical 4	Catastrophic 5
Frequent	5 tolerable	10 tolerable	15 un- acceptable	20 un- acceptable	25 un- acceptable



5					
Probable 4	4 acceptable	8 tolerable	12 un- acceptable	16 un- acceptable	20 un- acceptable
Occasional 3	3 acceptable	6 tolerable	9 tolerable	12 un- acceptable	15 un- acceptable
Unlikely 2	2 acceptable	4 acceptable	6 tolerable	8 tolerable	10 tolerable
Very Unlikely 1	1 acceptable	2 acceptable	3 acceptable	4 acceptable	5 tolerable

## 6 Relationships with other risk management processes

The safety risk management team may be separate from the security risk management team and the usability engineering team. Or they may be in a single team. In any cases, communication is required between safety, usability, and security.

### 6.1 Ranking system of safety risks when security breach is the hazardous phenomenon

According to Annex F of ISO 24971:2020, in case of security risks with impact on safety, the probability of risks can be split into:

- P1 = Probability that a vulnerability can be exploited by the threats (the hazardous situation),
- P2 = Probability that the hazardous situation (a vulnerability can be exploited by the threats) leads to a harm.


POSSIBILITY 1: Ranking system for security risk analysis based on CVSS

P1 can be estimated with the CSSS base score [0 ; 10]

Ranking	Definition	Probability (P1)
5	$8 \leq \text{CVSS base score} \leq 10$	Frequent (very high probability)
4	$6 \leq \text{CVSS base score} < 8$	Probable (high probability)
3	$4 \leq \text{CVSS base score} < 6$	Occasional (moderate probability)
2	$2 \leq \text{CVSS base score} < 4$	Unlikely (low probability)
1	$0 \leq \text{CVSS base score} < 2$	Very Unlikely (very low probability)

POSSIBILITY 2: Ranking system for security risk analysis

P1 can be estimated as equal to the probability of occurrence of the security risk as defined above.

	<b>Security Risk Management Plan of Paperless GMP Software</b>	PROTOCOL NO.
		EFFECTIVE DATE :
		PAGE NO.:

P2 is estimated with the scale:

Ranking	Definition	Probability (P2)
5	Frequent	Attack systematically or very often leads to harm
4	Probable	Attack could easily lead to harm in normal condition of use
3	Occasional	Attack could lead to harm in particular condition of use
2	Remote	There's a chance that the attack will lead to harm in device lifetime
1	Improbable	There's no chance that the attack will lead to harm in device lifetime

Then the total probability of a safety risk can be estimated as  $P = P1 \times P2$ .

Ranking	Definition	Description
5	Frequent	$20 \leq P1 \times P2 \leq 25$
4	Probable	$15 \leq P1 \times P2 < 20$
3	Occasional	$10 \leq P1 \times P2 < 15$
2	Remote	$5 \leq P1 \times P2 < 10$
1	Improbable	$0 < P1 \times P2 \leq 5$

## 6.2 Communication with safety risk management team

Communication with the safety risk management team shall be performed in a timely manner when:


- A security risk has a potential impact on safety,
- Security controls may affect safety,
- A security incident may affect safety.

In case of security incident, which may affect safety, the information shall be immediately reported to the person in charge of medical device reporting / materiovigilance.

## 6.3 Communication with usability engineering team

Communication with the usability engineering team shall be performed in a timely manner when:

- A security risk has a potential impact on usability,

	<b>Security Risk Management Plan of Paperless GMP Software</b>	PROTOCOL NO.
		EFFECTIVE DATE :
		PAGE NO.:

- A security control may affect or have an impact on usability.

When a security control has an impact on usability, the assessment of the effectiveness of the security control shall take account of results of usability assessment. Eg. The use scenario where the security control appears may be included in the summative evaluation.