

# **IT / OT Supplier Technical Security Standard**

## **MONDI Štětí a.s.**

**Classification: Public**

## Terminology

AT – Automation Solution  
APT – Advance Persistent Threat  
BPCS – Basic Process Control System  
CPU - Central Computing Unit  
CMDB – Configuration Management Database  
DB - database  
ESD – Emergency Shutdown System  
FAT - acceptance test before delivery  
FW - firmware  
HW - hardware equipment  
ICT - Information and Communication Technologies  
LAN - Local area network  
MFA – Multi Factor Authentication  
NTP – Network Time Protocol  
OT – Operational Technology  
OPC - open platform communication (former OLE for process management)  
PC - personal computer  
PIMS - process information management system  
RBAC – Role Based Access Control  
RDP - Remote Desktop Protocol  
SAT - Acceptance test after installation  
SNMP – Simple Network Management Protocol  
SW - Software equipment  
SIS – Safety Instrumented System  
VPN - virtual private network

## Introduction

This IT / OT Vendor Technical Security Standard (hereinafter referred as Standard) for Contractors and Vendors of MONDI Štětí, a.s. and Mondi Štětí White Paper s.r.o. (hereinafter referred to as the "Company"), contains a list of technical security requirements and design guidelines developed under IEC 62443 for OT environments (hereinafter referred to as "operating technologies") and IEC ISO 27001 and IEC ISO 27002 for IT environments. This Standard is mandatory for the Contractors or Vendors (hereinafter referred to as "Supplier").

### **The objective of this Standard is to:**

1. Ensure that prior to initiating any IT / OT system related procurement, strategic efforts are made to align Suppliers in the supply chain to security expectations, including the security engineering process which shall be followed, and the expected security requirements fulfilled.
2. Ensure that security clauses, specifications, and selected risk reduction measures in this Standard are incorporated/attached in all procurement contracts.

**This Standard is mandatory for the Suppliers of Company that supply IT / OT technologies for:**



- a) new DCS control systems implementation or changes, upgrades, innovations;
- b) new IT systems implementation or changes, upgrades, innovations;
- c) new connections to IT or OT systems;
- d) future procurements, that shall adopt secure development processes, including security functions in IT/ OT systems and components;

### Secure Engineering, Security-by-Design, Privacy-by-Design

Every new IT / OT systems bring security risks which must be assessed. Once a system has been risk assessed then any projects that might affect it need to be engaged so that security can be built into the project from an early stage – **Security-by-Design**. The objective of this Standard is to define security requirements for a 'green field' (new project site) or a 'brown field' (retrofitting) that shall build security requirements into the design and build process from an early stage. The assurance of these requirements should be assessed throughout the project life cycle of IT and OT systems.

**Privacy-by-Design** means that when a system or service includes choices for the individual on how much personal data he/she shares with others, the default settings should be the most privacy friendly ones. Privacy by Design and Privacy by Default is a new legal requirements under the GDPR, these concepts shall be met. Considering privacy from the start of the development process is essential to address privacy successfully.

**Secure-by-Default** is based primarily on the concept of Defense in Depth, which is a common term applied to describe the goal of a practical multi-layered security implementation. This Standard also provides guidelines for creating a minimal attack surface, a standard installation and securing the default and system settings.

### Communication with Supplier – Responsible Person

The Company's **Responsible Person** is a person who is entrusted and appointed by the Company, and who is managing projects, supplies or services with the Contractor. Responsible Person is responsible for managing all exceptions of this Policy.

The Responsible Person at the Company is usually:

- Project Manager responsible for a new supply of IT / OT systems or services,
- E&I Manager;
- Maintenance Department Manager;
- IT Manager;
- Process control specialist
- IT Specialist;
- CISO for specific cyber security standards & requirements clarification

### Procurement Language

This Technical Security Standard (hereinafter "Standard") provides baseline cybersecurity procurement language that is representing minimum security requirement of the Company that shall be fulfilled by the Supplier.

Readers of this document have the responsibility of ensuring that actions taken during the procurement process comply with this Standard and local regulations. In addition to the language included in this document, acquired products and services should conform to the applicable **"IT / OT Supplier Security Policy"**.

Supplier's product life cycle should cover a product's design, development, manufacture, storage, delivery, implementation, maintenance, and disposal. A properly designed and implemented IT / OT system should lower the cyber risk that the Supplier's products would present major cybersecurity challenges for the Company.



**Table 1:** Definitions for the Different Categories of Procurement Language Stakeholders:

Procurement Language Stakeholder	Definition
<b>The Company (Acquirer)</b>	Stakeholder that acquires or procures a product or service.
<b>Supplier</b>	Organization or individual that enters into an agreement with the Acquirer or Integrator for supplying a product or service. This includes all Suppliers in the supply chain.
<b>Integrator</b>	An organization that develops systems and components for deployment or customizes (e.g., combines, adds, or optimizes) components, systems, and corresponding processes.

**Table 2:** Table 2. Definition of Procurement Language Terminology

Wording	Definition
<b>“shall” and “shall not”</b>	The terms “shall” and “shall not” indicate that the procurement language element in which these terms appear is to be strictly followed if the Supplier and Company agree to adopt the language in their procurement contract.
<b>“should” and “should not”</b>	The terms “should” and “should not” indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.
<b>“may”</b>	The term “may” indicates a course of action permissible within the limits of the document.
<b>“procured product”</b>	The term “procured product” may refer to the hardware, software, and firmware that compose the delivered IT / OT system, or a component thereof, that is being acquired through the procurement process. This may also refer to support and maintenance services that are being acquired through the procurement process.

### Applicability of Procurement Language

Unless otherwise specified, the procurement language in this document is intended to apply “at the point of delivery” of the Procured Product ( IT /OT systems or components). Service and support provided by the Supplier may apply, as indicated, well after the delivery of the Procured Product. Some aspects of the Supplier’s product life cycle security program apply well before and well after the delivery of the product.

# General Security Design Specifications

## 1. Software and Hardware

ID	Security Requirement	Description
1.1	Preferred Technologies for OT networks	Industrial protocol communication requirements must be communicated with Responsible Person prior OT technology deployment.  Preferred networking technology is Cisco.  Preferred intercommunication protocol is OPC
1.2	Preferred Technologies for IT networks	CISCO networking platform is preferred.
1.3	Operating Systems	Delivered Operating system and SW components shall be supported and available at least 5 years after delivery, ideally 8+ years  The Supplier should propose Long-Term Servicing Branch (LTSC/LTSB editions) for Windows 10 Operating Systems
1.4	Virtualization	VMware virtualization platforms (ESXi 6.0 and vSphere 6.0)
1.5	Servers	The Supplier shall supply components to be able: <ul style="list-style-type: none"> <li>• HW Components shall be hot-plug/hot-swap replaceable in case of failure HW solution with no single point of failure architecture for business critical operation areas</li> <li>• System shall be manageable remotely (including cold start / stop)</li> <li>• Server hard disks should be encrypted (if technically possible)</li> </ul>
1.6	Workstations /Operator Station	The Supplier shall in OT: <ul style="list-style-type: none"> <li>• Ensure that OT operator can't escape it's privileges "operator jailbreakout" on the operator station and shall not be able to run privilege escalation attack to get admin rights.</li> <li>• Operator workstation should have in-line backup power (UPS) at least for 20 mins. See the standard "ST20.04"</li> <li>• Operator station should have an OPC client to TIS (signalization specification is negotiated before the installation)</li> </ul> The Supplier shall in IT: <ul style="list-style-type: none"> <li>• Supply PC desktop computers and laptops according to request by IT department.</li> </ul>
1.7	Thin Clients	The Supplier shall supply the following functions for Thin clients: <ul style="list-style-type: none"> <li>• Technical capability to remotely connect operator stations</li> </ul>

		<ul style="list-style-type: none"> <li>• RDP protocols support</li> <li>• SSL/TLS encryption support</li> <li>• USB peripherals blocking capability</li> <li>• Disable functionality for WI-FI</li> <li>• Local access for standard “thin” clients</li> </ul>
<b>1.8</b>	Engineering Stations (EWS)	<ul style="list-style-type: none"> <li>• EWS Engineering Station is a critical DCS component and must be adequately secure against cyber attacks ( by hardening)</li> <li>• The Supplier may recommend Application Whitelisting (AWL) software that is certified for EWS. If AWL is delivered, it shall be enabled.</li> <li>• The Supplier is required to design a secure OT architecture so that it can logically separate EWS by VLANs from other DCS components.</li> <li>• The Supplier shall harden EWS and turn off insecure protocols and services (see hardening policy below) 1.20.</li> </ul>
<b>1.9</b>	Safety Instrumented System SIS /SRS / ESD	<ul style="list-style-type: none"> <li>• The Supplier shall follow IEC 61508 and IEC 61511 safety measure and cyber security recommendations of automation vendors</li> <li>• Security certifications such as Achilles I and Achilles II and above, ISASecure Embedded Device Security Assurance, ISASecure EDSA, IEC 62443-4-1, IEC 62443-4-2, should be considered when procuring SIS</li> <li>• SIS shall follow an “Absolute Air Gap” from BPCS to satisfy the security measure if possible. If there is an interconnection needed between SIS and BPCS, it must be justified by detailed risk analysis.</li> <li>• Secure-by-Default - after installation the system by default presents a minimal attack surface. This is accomplished by secure default configuration settings and by automatically disabling unused functions.</li> <li>• Remote access to SIS is strictly forbidden.</li> </ul>
<b>1.10</b>	Databases	<ul style="list-style-type: none"> <li>• Oracle and MS SQL is preferred</li> </ul>
<b>1.11</b>	High-Availability and Resiliency	<ul style="list-style-type: none"> <li>• No Single Point of Failure for business critical solutions</li> </ul>
<b>1.12</b>	Performance and Capacity	<p>The Supplier shall ensure that supplied components (where technically possible):</p> <ul style="list-style-type: none"> <li>• The initial free CPU capacity shall be higher than 40%</li> <li>• The initial free Memory capacity shall be higher than 40%</li> <li>• Free capacity shall remain for 3 years since start of the system</li> <li>• Latencies, delays, jitter shall not cause disruption of business or industrial processes of implemented IT</li> </ul>

		<p>/ OT systems. (these parameters shall be negotiated with the Company)</p> <ul style="list-style-type: none"> <li>• Exceptions from these requirements shall be communicated with Responsible Person</li> </ul>
<b>1.13</b>	HW and SW Compatibility	The Supplier shall supply compatible HW and SW in order to achieve interoperability with other systems. Responsible Person of Company shall verify compatibility requirements.
<b>1.14</b>	HW and SW Technical Support	The Supplier shall supply HW and SW and spare parts that shall have technical support for at least 5 years, preferable 8 years and more.
<b>1.15</b>	Electrical Switchgear	The Supplier shall supply components compatible with Company standards as defined in "ST20".
<b>1.16</b>	Documentation	The Supplier shall provide summary documentation of the Procured Product's security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings.
<b>1.17</b>	License Management	<p>The Supplier shall provide all related licenses for the Procured Product and clearly defined licensing policy of the technology supplied.</p> <p>IT/OT technologies shall be by default licensed after the delivery to the Company.</p> <p>All specific SW or HW licenses have to be finally registered to Mondy .</p> <p>All licenses shall be indicated as separated item in an invoice.</p>
<b>1.18</b>	Secure Supply Chain	The Supplier shall establish, document, and implement risk management practices for IT / OT supply chain delivery of hardware, software, and firmware. The Supplier shall use trusted channels to ship critical IT / OT components in order to prevent tampering and manipulation.
<b>1.19</b>	Detection of Unauthorized Delivery	The Supplier shall demonstrate a capability for detecting unauthorized access throughout the delivery process.
<b>1.20</b>	Security Hardening	<p>The Supplier shall remove all software components that are not required for the operation and/or maintenance of the Procured Product. If removal is not technically feasible, then the Supplier shall disable software not required for the operation and/or maintenance of the procured product. This removal shall not impede the primary function of the procured product. If software that is not required cannot be removed or disabled, the Supplier shall document a specific explanation and provide risk mitigating recommendations and/or specific technical justification. The Supplier shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but not be limited to:</p> <ul style="list-style-type: none"> <li>• Gaming software and device drivers for product components not procured/delivered</li> <li>• Messaging services (e.g., email, instant messenger, peer-to-peer file sharing)</li> <li>• Source code or libraries not necessary for operation purposes</li> <li>• Software compilers for programming languages that are not used for operational purposes</li> </ul>

		<ul style="list-style-type: none"> <li>• Unused networking and communications protocols (DHCP, TELNET, IPv6, etc.)</li> <li>• Unused administrative utilities, diagnostics, network management, and system management functions</li> <li>• Backups of files, databases, and programs used only during system development.</li> <li>• All unused data and configuration files</li> <li>• NTLM version 2 and above must be used for Windows OS</li> </ul>
<b>1.21</b>	Software Security-by-Default	<p>The Supplier shall provide Security-by-Default in software and ensure protection against:</p> <ul style="list-style-type: none"> <li>• Buffer overflows, in which input fields are populated with long data sequences that overflow program buffers, often yielding program controls to the remote user (providing a useful command prompt in some cases).</li> <li>• Data insertion and injection, in which input fields are populated with control or command sequences embedded in various ways that are nevertheless accepted by the application, or possibly passed to the OS, and that allow privileged malicious and unauthorized programs to be run on the remote system.</li> </ul>
<b>1.22</b>	Secure Programming Practices	<p>The Supplier shall supply software that includes the following security embedded imperatives:</p> <ul style="list-style-type: none"> <li>• Check inputs for reasonable values</li> <li>• Encrypt data files</li> <li>• Understand security impacts of OSs and other third-party libraries</li> <li>• Make sure OSs and other third-party libraries have an update policy</li> <li>• Forbid buffer overflow</li> <li>• Verify log files are unalterable</li> <li>• Use end-to-end authentication and integrity checks on process-to-process data communications</li> <li>• Verify no clear-text passwords or encryption keys are embedded in the code or communicated</li> <li>• Use secure design and code reviews.</li> </ul>

## 2. PHYSICAL SECURITY

ID	Security Requirement	Description
<b>2.1</b>	Lockable Enclosures and Racks	Supplied racks shall be lockable or have locking enclosures or for IT / OT systems and its system components (e.g., servers, clients, and networking hardware) and for the systems used to manage and control physical access (e.g., servers, lock controllers, and alarm control panels).
<b>2.2</b>	Tamper Detection	The Supplier should provide a method for tamper detection on lockable or locking enclosures. If a physical security and monitoring system is used, tamper detection shall be compatible.



2.3	Interoperability	The Supplier shall implement physical security controls at the Company's premises ensuring that new physical security controls do not hamper current physical security controls and their operations.
2.4	Two-Factor Authentication	If specified by the Company, the Supplier should provide two-factor authentication for physical access control. (e.g. server rooms access control)
2.5	Security Perimeter Assessment for Data Centers	The Supplier shall provide a physical security recommendations and assessment as specified by the Company and relevant to the procurement that defines the security perimeter physical access points and controls needed at each access point. (e.g. when building new technical rooms or data centers).
2.6	Alarm System	If specified, the Supplier shall coordinate with the Company when installing and using physical intrusion alarm systems as defined and specified by the Company.
2.7	CCTV	If specified, the Supplier shall coordinate with the Company when installing and CCTV (camera systems) as defined and specified by the Company.
2.8	Environmental Sensors	If specified, the Supplier shall coordinate with the Company when installing and environmental sensors (humidity, temperature, seismic, water leakage etc.) as defined and specified by the Company.
2.9	Physical Communication Channels	The Supplier shall verify and provide documentation that physical communication channels are secured from physical intrusion. (e.g. secure cabling standards).  Panduit and Belden are preferred cabling solutions..
2.10	Documentation and Testing	The Supplier shall test and provide documentation that implemented physical security controls are completed and working.
2.11	Lockable Enclosures and Racks	Supplied racks shall be lockable or have locking enclosures or for IT / OT systems and its system components (e.g., servers, clients, and networking hardware) and for the systems used to manage and control physical access (e.g., servers, lock controllers, and alarm control panels).
2.12	Tamper Detection	The Supplier should provide a method for tamper detection on lockable or locking enclosures. If a physical security and monitoring system is used, tamper detection shall be compatible.

### 3. ACCESS CONTROL

ID	Security Requirement	Description
3.1	Least Privilege Rule	The Supplier shall configure each component of the procured product to operate using the principle of least privilege. This includes operating system permissions, file access, user accounts, application-to-application communications, and all relevant devices in IT / OT systems.
3.2	Privilege Access Management	The Supplier shall configure and document options for defining access and security permissions, user accounts,

		and applications with associated roles. The Supplier shall configure these options, as specified by the Company.
<b>3.3</b>	Privilege Levels	The Supplier shall provide technical capability that a role based model must distinguish between various access levels (privileges) for end users and for privileged users (e.g. system administrators).
<b>3.4</b>	Role Based Access Control (RBAC)	The Supplier shall provide user accounts with configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used. Every user must have unique identifier and password configured unless otherwise specified by the Company.
<b>3.5</b>	Privilege Escalation Rule	The Supplier shall provide a method for protecting against unauthorized privilege escalation.
<b>3.6</b>	Two-factor (2FA) and Multi-Factor Authentication (MFA)	The Supplier solutions shall be involving 2FA and MFA (physical and logical mechanisms) when requested by Company and be compatible with the Company's actual implementation of multifactor authentication methods.
<b>3.7</b>	Single Sign-On Support	The Supplier solutions shall be involving SSO when requested by Company and be compatible with the Company's actual implementation of SSO authentication methods.
<b>3.8</b>	Session and Console Security	The Supplier shall configure the procured product such that when a session or interprocess communication is initiated from a less privileged application, access shall be limited and enforced at the more critical side. (e.g. by ACL on VTY terminal).
<b>3.9</b>	Session Encryption	The Supplier shall provide an appropriate level of protection (e.g., encryption and digital signing) for the session, as specified by the Company, commensurate with the technology platform, communications characteristics, and response time constraints. Secure protocols such as SSHv2, SFTP, HTTPS, TLS shall only be used. Insecure protocols must be documented to Company.
<b>3.10</b>	Concurrent Logins	Unless specifically requested by the Company, the Supplier shall not allow multiple concurrent logins using the same authentication credentials (generic accounts), allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous/guest logins.
<b>3.11</b>	Logout Mechanism	The Supplier shall provide account-based and group-based configurable session-based logout and timeout settings. Alarm stations and human-machine interfaces shall not be configured for automatic logouts.
<b>3.12</b>	Unauthorized Access / Covert Channel	The Supplier shall verify and ensure for the procured product, confirming that unauthorized connections or logging devices are not installed (e.g., key loggers, Remote Access Trojans, Cameras, Microphones, Spy devices etc.), as specified by the Company.
<b>3.13</b>	Infrastructure Access Controls	The Supplier shall deliver an IT / OT system or product that enables the ability for the Company to configure its components to limit access to and from specific locations (e.g., network segments, security zones, business networks, and demilitarized zones [DMZs]) on the network to which the

		components are attached, where appropriate, and provide documentation of the product's configuration as delivered.
--	--	--

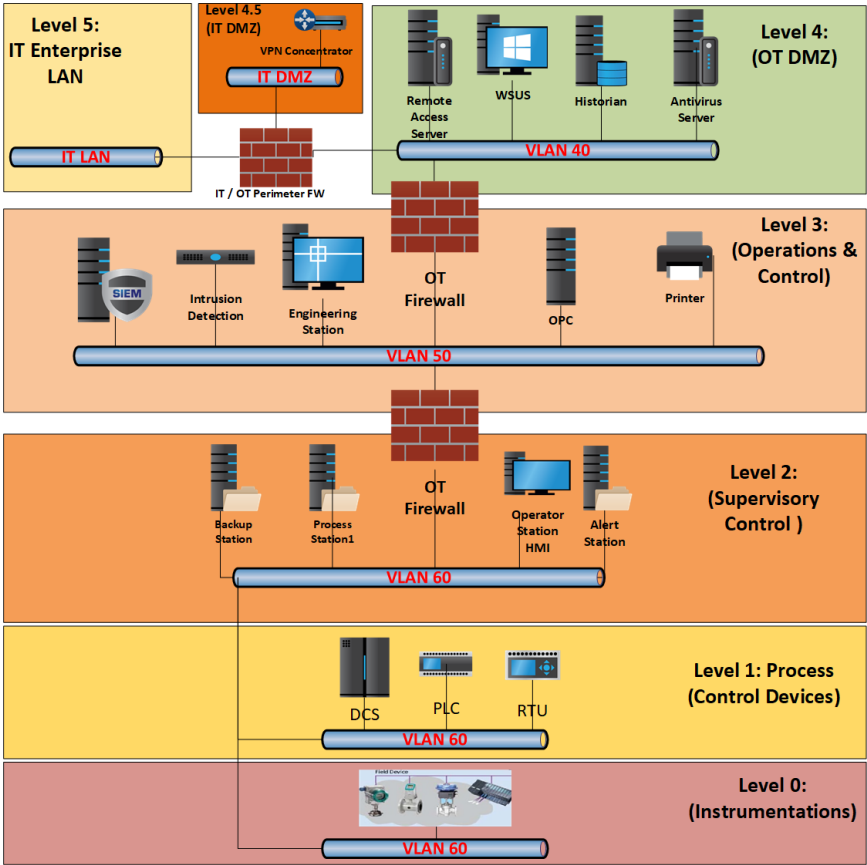
#### 4. ACCOUNT MANAGEMENT

ID	Security Requirement	Description
4.1	Default and Service Accounts	The Supplier shall change default account settings to Company-specific settings (e.g., length, complexity, history, and configurations) or support the Company in these changes. The Supplier shall not publish changed account information. The Supplier shall provide new account information to the Company via a protected mechanism.
4.2	Default and Service Accounts Exceptions	The Supplier shall document all account exceptions (including, but not limited to, application hardwired, service, generic and/or default) that need to be active for proper operation of the procured product. Exceptions are strongly discouraged.
4.3	Accounts Hardening	Prior to delivery of the procured product to the Company, the Supplier shall remove or disable any accounts that are not needed for normal or maintenance operations of the IT / OT systems or products.
4.4	Credentials Protection	The Procured Product shall not permit user credentials to be transmitted or shared in clear text. The Supplier shall not store user credentials in clear text unless the Supplier and Company agree that this is an acceptable practice for the procured product given the protection offered by other security controls. The Supplier shall only allow access protocols that encrypt or securely transmit login credentials (e.g., tunneling through Secure Shell Terminal Emulation [SSH], Transport Layer Security [TLS]).
4.5	Account Management	The Supplier should provide Procured Product with technical capability for a centralized and local account management capability. Centralized account management should support Authentication, Authorization, Accounting capabilities offered by TACACS+ and/or RADIUS protocol.
4.6	Redundant Accounts	The Supplier shall ensure that no redundant accounts are configured in Procured Product.
4.7	User Account Deletion & Logging	The Procured Product shall have the technical capability to generate an audit log report after the completion of integration/maintenance activities that shows that accounts used to support these activities have been removed from IT / OT Systems if they are no longer needed.
4.8	User Account Expiration	The Procured Product shall have technical capability to ensure that login or/and user accounts, and other accounts required for essential functions have expiration timer functionality.
4.9	Password Management Capabilities	The Supplier shall provide a Procured Product that has configurable account password management that technically allows for, but is not limited to, the following: <ul style="list-style-type: none"> <li>• Changes to passwords (including default passwords)</li> <li>• Selection of password length</li> </ul>

		<ul style="list-style-type: none"> <li>• Frequency of change</li> <li>• Setting of required password complexity</li> <li>• Number of login attempts prior to lockout Inactive session logout</li> <li>• Screen lock by application (except OT)</li> <li>• Derivative use of the user name</li> <li>• Denial of repeated or recycled use of the same password</li> </ul>
<b>4.10</b>	Password Protection	The Procured Product shall have a technical capability to protect passwords, including not storing passwords in clear text and not hardcoding passwords into software or scripts by using hashing mechanisms, salt & pepper tokenization etc.

## 5. NETWORK SECURITY

ID	Security Requirement	Description
<b>5.1</b>	Network Segmentation	The Procured Product or IT / OT platform shall follow Security-by-Design (ISA 99, Purdue Model for OT) and support network segmentation and security zoning. The Supplier shall provide a method to restrict communication traffic between different network security zones. The Supplier shall provide documentation on any method or equipment used to restrict communication traffic.
<b>5.2</b>	Secure Reference Architecture	The Supplier shall implement the following secure architecture and segmentation in OT:

		
5.3	DMZ	The Supplier shall provide or utilize an existing security-isolated environment between IT / OT environments (e.g., using a demilitarized zone [DMZ] or an equivalent or a superior form of security isolation) for the communications. The Company will provide guidance which server shall reside in DMZ.
5.4	Traffic and Protocol Flow	The Supplier shall provide information on all communications (e.g., protocols) required between network security zones, whether inbound or outbound, and identify each network component of the procured product initiating communication.
5.5	Firewall	<p>By default Firewalls are provided by the Company, the Supplier shall not install any firewalls in IT / OT infrastructure but shall provide particular traffic flows for its technological platforms.</p> <p>The Company is responsible for appropriate firewall rule set up and firewall configuration.</p> <p>The Company implies that the basis of the firewall rule sets shall be “deny all,” with exceptions explicitly identified by the Company.</p>
5.6	Equipment Access	The Supplier shall provide to the Company all equipment accesses, including service/emergency, to all supplied IT / OT components.
5.7	Wireless Interoperability	The Supplier shall document specific protocols and other detailed information required for wireless devices to communicate with the IT / OT systems, including other wireless equipment that can communicate with the Company-owned devices.
5.8	Wireless Standards	The Supplier shall document that the wireless technology and associated devices comply with standard operational and security requirements specified in applicable wireless standard(s) or specification(s) (e.g., applicable IEEE standards, such as 802.11).

5.9	Wireless Security	<p>The Supplier shall ensure that Wi-Fi is using secure protocols, encrypted and authenticated, with the following parameters in the IT / OT networks:</p> <p>For the <b>IEEE 802.11</b> family of protocols:</p> <ul style="list-style-type: none"> <li>• Encryption mechanism: WPA version 2, WPA version 3 and above;</li> <li>• Authentication: <ul style="list-style-type: none"> <li>◦ 802.1x is preferred in Enterprise mode,</li> <li>◦ Pre-shared key: 12 characters at least, use special characters, numbers, capital letters</li> <li>◦ If mutual device authentication is required; use EAP/LEAP</li> </ul> </li> <li>• IPSec hash algorithm <ul style="list-style-type: none"> <li>◦ For the IEEE 802.15.2-Bluetooth:</li> <li>◦ For the IEEE 802.15.4 - ZigBee, ISA 100.11.a, Wireless HART:</li> </ul> </li> <li>• Encryption algorithm: 128-bit or higher.</li> <li>• Use MAC address filtering of subscribers if possible</li> <li>• Bluetooth: All security mechanisms (authentication and encryption) are turned off in Bluetooth and they must be enabled during implementation.</li> </ul> <p>Wireless security logging:</p> <ul style="list-style-type: none"> <li>• Authentication failed</li> <li>• Failed access to the network</li> <li>• Default passwords are forbidden and has to be changed</li> </ul>
5.10	GSM modems	<ul style="list-style-type: none"> <li>• Disable 2G networks (GSM, GPRS y EDGE): they are insecure networks by default.</li> <li>• Remote access is solely managed by Company. The Supplier shall not install any GSM, Satellite or any other modems on its own.</li> </ul>
5.11	IoT and IIoT	<ul style="list-style-type: none"> <li>• IoT and IIoT technology should use Narrow Band technology.</li> </ul>
5.12	IP addressing	<ul style="list-style-type: none"> <li>• The Company will provide IP addresses ranges</li> </ul>

## 6. REMOTE ACCESS SECURITY

ID	Security Requirement	Description
6.1	Remote Access	<p>The procured product for remote VPN communication (e.g., VPN concentrator) shall provide end-to-end protection (e.g., end-to-end encryption) of the data in transit. This shall address confidentiality and/or integrity, as specified by the Company.</p> <p><b>Site-to-site VPN and Client VPN parameters:</b></p> <ul style="list-style-type: none"> <li>• IPSec encryption algorithm: AES 192, 256 and above;</li> <li>• IPSec hash algorithm: SHA-2, SHA-3 with key length 224 and higher;</li> <li>• Diffie-Hellman group: Group 7 (163-bit elliptical curve), Group 14 (2048-bit modulus) and higher with Perfect Forward Secrecy (PFC) enabled; SW and HW allow;</li> <li>• Preshared Key: at least 12 alphanumeric characters with special characters "! @ # \$ % ^ &amp; * ( ) _";</li> <li>• Certificate validation: RSA or DSA (PKCS7 or X.509);</li> </ul> <p><b>Web SSL VPN:</b></p> <ul style="list-style-type: none"> <li>• SSL version 3;</li> <li>• Session timeout) 10 min;</li> </ul>

<b>6.2</b>	Remote VPN Traffic Restrictions	The Supplied Product shall provide a method to restrict communication traffic between different networks and security zones. The Supplier shall provide documentation on any method or equipment used to restrict communication traffic.
<b>6.3</b>	Inbound / Outbound Connections	The Procured Product shall provide information on all communications (e.g., protocols) required between his source IPs and destination IPs, both inbound or outbound, and identify each network component of initiating communication.
<b>6.4</b>	Monitoring Capabilities	The Procured Product shall provide a technical capabilities for network traffic monitoring, filtering, and alarming (e.g., alarms for unexpected traffic or cyber threats through network security zones) and provide filtering and monitoring rules.

## 7. INTRUSION DETECTION AND MONITORING

ID	Security Requirement	Description
<b>7.1</b>	Host Intrusion Detection Systems (HIDS)	The Supplier shall provide either a configured HIDS or the information needed for the Company to configure the HIDS.
<b>7.2</b>	Implementation	The Supplier shall implement or recommend a configuration for the HIDS in a manner that adheres to requirements for the Company's operating system functions or business / industrial objectives.
<b>7.3</b>	Integration	Procured Product shall have technical capabilities to be integrated with Company's health check monitoring.
<b>7.4</b>	Auditing & Logging	The Procured Product shall embed the auditing and logging provisions to the HIDS.
<b>7.5</b>	Network Intrusion Detection Systems (NIDS)	The Supplier may recommend a placement(s) of the NIDS sensors to provide appropriate monitoring for the IT / OT system network.

## 8. LOGGING

ID	Security Requirement	Description
<b>8.1</b>	Logging	<p>The Procured Product shall provide logging capabilities or the ability to support the Company's existing logging system. Logging capabilities provided by the Supplier shall be configurable by the Company and support the Company's security auditing requirements. As specified by the Company, the procured product shall cover the following events, at a minimum (as appropriate to their function):</p> <ul style="list-style-type: none"> <li>• Information requests and server responses</li> <li>• Successful and unsuccessful authentication and access attempts</li> <li>• Account changes</li> <li>• Privileged use</li> </ul>



		<ul style="list-style-type: none"> <li>• Application start-up and shutdown</li> <li>• Application failures</li> <li>• Major application configuration changes</li> </ul> <p>The Supplier shall provide a list of all log management capabilities that the procured product is capable of generating and the format of those logs. This list shall identify which of those logs are enabled by default.</p>
<b>8.2</b>	Log Retention & Forwarding	The Procured Product shall have a technical capability for collecting and storing (e.g., transfer or log forwarding) security log files.
<b>8.3</b>	Log Time Stamp	The Procured Product shall have technical capability for time stamp audit trails and log files.
<b>8.4</b>	NTP time synchronization	The Supplier shall configure the NTP protocol for all components in the delivery. The IP address of the NTP server is provided by the Company.

## 9. BACKUP AND RESTORE

ID	Security Requirement	Description
<b>9.1</b>	Backup	The Supplied Product shall provide backup and restore technical capabilities.
<b>9.2</b>	Backup Interoperability	The Company uses centralized and standardized backup system that shall be compatible with Procured Product. Responsible Person of the Company should provide more details.
<b>9.3</b>	Backup Encryption	The Supplied Product should support encryption of backup data. AES 128 bits and higher is recommended.
<b>9.4</b>	Procedures	The Supplier shall provide backup and restore procedures of the Procured Product which includes RTO and RPO parameters recommended by the Supplier.
<b>9.5</b>	Backup Documentation	The Supplier shall provide documentation of Procured backup and restore product.

## 10. VULNERABILITY MANAGEMENT

ID	Security Requirement	Description
<b>10.1</b>	Vulnerability Capabilities	In the time of delivery, the Supplier shall identify and correct known cybersecurity weaknesses and vulnerabilities.
<b>10.2</b>	Vulnerability Scanning	The Company will scan for IT and OT system vulnerabilities during the SAT testing. The Supplier is obligated to mitigate all security findings detected by scanner in the reasonable period of time.



## 11. PATCH MANAGEMENT

ID	Security Requirement	Description
11.1	Patch Management	<p>The Supplier shall provide documentation of its patch management program and update process (including third-party hardware, software, and firmware).</p> <p>This documentation shall include resources and technical capabilities to sustain this program and process. This includes the Supplier's method or recommendation for how the integrity of the patch is validated by the Company. This documentation shall also include the Supplier's approach and capability to remediate newly reported zero-day vulnerabilities.</p>
11.2	Patch Availability	<p>The Supplier shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses as soon as possible. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates.</p>
11.3	Firmware Patches	<p>The Procured Product shall be delivered with the latest firmware security patches.</p>
11.4	Operating System Patches	<p>The Procured Product shall be delivered with the latest Operating Systems security patches.</p>
11.5	Centralized WSUS management	<p>The Company should recommend centralized WSUS patching management for IT / OT environments.</p>

## 12. ANTIVIRUS PROTECTION

ID	Security Requirement	Description
12.1	AV / Malware Detection	<p>The Supplier must deploy Antivirus solution based on requirements of the Company.</p> <p>The Procured Product shall provide a host-based malware detection capability for Windows OS stations. It shall quarantine (instead of automatically deleting) suspected infected files.</p> <p>Supplier shall provide guidance on malware detection and configuration settings (including scanning exceptions) that will work with Supplier products.</p> <p>The Supplier shall provide an updating scheme for malware signatures. The Supplier shall test and confirm compatibility of malware detection application patches and upgrades.</p>
12.2	AV Automatic Scanning	<p>The Company implies that automatic scanning shall run on weekly basis.</p>

### 13. REMOVABLE MEDIA

ID	Security Requirement	Description
13.1	Peripherals Blocking	<p>The Supplier shall remove and/or disable, through software, physical disconnection, or engineered barriers, all services and/or ports in the procured product not required for normal operation, emergency operations, or troubleshooting.</p> <p>This shall include communication ports and physical input/output ports (e.g., USB ports, CD/DVD drives, video ports, and serial ports). The Supplier shall provide documentation of disabled ports, connectors, and interfaces.</p>
13.2	OT Operator Stations	The Supplier shall block USB peripheral for all OT operator stations, which are running under user privileges.
13.3	Re-enable Blocking Capability	The Supplier shall configure the Procured Product to allow the Company the ability to re-enable ports and/or services if they are disabled by software.

### 14. SECURE SYSTEM DEVELOPMENT PRACTICES

ID	Security Requirement	Description
14.1	Secure System Development Life Cycle (SDLC)	The Supplier shall provide summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided IT / OT system hardware, software, and firmware.
14.2	Secure Software Development	<p>The Supplier shall follow industry best practices for application security such as OWASP, and these shall include:</p> <ul style="list-style-type: none"> <li>• Encode request/response</li> <li>• Use HTTPS for domain entries</li> <li>• Use only current encryption and hashing algorithms</li> <li>• Do not allow for directory listing</li> <li>• Do not store sensitive data inside cookies</li> <li>• Check the randomness of the session</li> <li>• Set secure and HttpOnly flags in cookies</li> <li>• Use TLS not SSL</li> <li>• Set strong password policy</li> <li>• Do not store sensitive information in a form's hidden fields</li> <li>• Verify file upload functionality</li> <li>• Set secure response headers</li> <li>• Make sure third party libraries are secured</li> <li>• Hide web server information</li> </ul>
14.2	Quality Control	The Supplier shall provide a Quality Assurance program and validate that the software and firmware of the Procured Product have undergone Quality Control testing.

## 15. ACCEPTANCE PROCESS OF DELIVERED SOLUTIONS AND SERVICES

ID	Security Requirement	Description
15.1	Acceptance Process	<p>The Supplier shall execute SAT / FAT and cooperate with Responsible Person and consider for inclusion in acceptance tests which include:</p> <ul style="list-style-type: none"> <li>• Security configuration (e.g. testing of firewalls, whitelisting and anti-malware)</li> <li>• Software review</li> <li>• Vulnerability assessment of the whole system</li> <li>• Failover/ disaster recovery testing</li> <li>• Backup and restore testing</li> <li>• Patch and update testing</li> <li>• User accounts</li> <li>• Remote access testing</li> <li>• Performance testing</li> <li>• System hardening assurance (e.g. penetration testing)</li> <li>• Ability to monitor the system (e.g. store and retrieve system logs).</li> </ul>
15.1	IT / OT Systems Handover Process	<p>As part of the process of handing over the systems to the Responsible Person of the Company all the associated process and procedures that are needed to support the security framework of the system need to be finalized and embedded into business as usual activities, these shall be include processes and procedures for:</p> <ul style="list-style-type: none"> <li>• Account management and authentication</li> <li>• Monitoring system logs</li> <li>• Maintenance routines</li> <li>• Firewalls management and monitoring</li> <li>• Anti-virus deployment and assurance</li> <li>• Response and continuity plans</li> <li>• Backup and Restore procedure</li> <li>• Fail-over testing</li> <li>• Patching processes</li> <li>• System isolation (segmentation)</li> <li>• Contingency procedures</li> <li>• Confirmation of all software on hard disks and firmware</li> <li>• Up to date system documentation (network diagrams including links to IT / OT systems)</li> <li>• Results of factory acceptance tests (FAT ) and commissioning tests.</li> </ul>

## 16. PROBLEM REPORTING

ID	Security Requirement	Description
16.1	Problem Reporting Process	The Supplier shall provide a secure process for users of the Company to submit problem reports and remediation

		requests. This process shall include tracking history and corrective action status reporting.
<b>16.2</b>	Submitting a Problem	Upon the Company submitting a problem report to the Supplier, the Supplier shall review the report, develop an initial action plan], and provide status reports of the problem resolution to the Company.

MONDI Štětí, a.s. and Mondí Štětí White Paper s.r.o. reserve the right to amend and amend this Standard with the obligation to inform the Supplier of any such change. The date of the announcement of the amendments to the Standard, or later on the date stated in the notice, becomes binding Standard as amended and supplemented.

Effective date: 1. October 2019