

Istruzioni (ITA)

1- Compilare la tabella "Info Generali" (propria parte di competenza: Utilizzatore / Fornitore / Ing. Clinica)

2- Compilare la tabella "CyberSec_DataProt_Checklist"

1- compilare le colonne "RISPOSTA (SI / NO)" e "CAMPO NOTE"

2- i campi che appaiono in giallo sono obbligatori

3- i campi in bianco sono facoltativi

4- se un campo diventa **rosso**, non era da compilare

5- SCRIVERE la risposta in OGNI SINGOLA cella, o utilizzare il menu a tendina della cella

6- **ATTENZIONE: NON copiare e NON trascinare le risposte da altre celle: si perderebbero i controlli colorati delle celle, di aiuto alla compilazione**

Instructions (ENG)

1- Fill-in your card (Supplier / User / Biomedical Dep.) in the sheet 'Info Generali'

2- Fill-in the sheet 'Cybersec & Dataprot Checklist'

1- fill in the columns 'RISPOSTA / ANSWER (SI/NO)' and 'CAMPO NOTE / COMMENTS'

2- yellow fields are mandatory

3- blank fields are optional

4- if a field turns **red**, it was not to be completed

5- WRITE the answer in EACH SINGLE cell, or use the cell drop down menu

6- PLEASE PAY ATTENTION: DO NOT copy and DO NOT drag answers from other cells: you'll lose the colored controls of the cells, that helps the correct completion of the form

Fornitore (Supplier)	
Apparecchiatura <i>(Equipment)</i>	
Modello <i>(Model)</i>	
Produttore <i>(Manufacturer)</i>	
Fornitore <i>(Supplier)</i>	
Contatto Fornitore (nome, cell., mail) <i>Supplier contact (name, telephone number, e-mail)</i>	

Info Utilizzatore	
Area Clinica / Area Ricerca	
Unità Operativa	
Localizzazione dell'apparecchiatura	
A cosa serve?	
Contatto Utilizzatore (nome, tel., mail)	

Ingegneria Clinica	
Inventario SIC	
Data di installazione prevista / data di collaudo già effettuato	
Forma di presenza (acquisto, comodato, visione, prot. di ricerca, locazione, donazione, noleggio, acquisto di terzi)	
Note aggiuntive	
Ticket NCIS	
Presenza di rete	
Contatto SIC (nome, tel., mail)	

I.R.C.C.S. Ospedale San Raffaele Gruppo San Donato		Servizio di Ingegneria Clinica		Inv.	mod.			
CYBERSECURITY & DATA PROTECTION CHECKLIST Apparecchiature Elettromedicali e da Laboratorio				Note	RISPOSTA/ ANSWER (SI / NO)	CAMPO NOTE / COMMENTS	Fornit ore	Utilizz atore
A1 SICUREZZA GENERALE DI SISTEMA							X	X
A1.1 Architettura hw e sw							X	
A1.1	Descrivere l'architettura del sistema .1 Indicare se apparecchiatura singola, oppure la lista dei singoli apparati IT (e relative connessioni)						X	
A1.1	Sistema Operativo installato .2 (release esatta, per ogni apparato IT)						X	
A1.1	Il Sistema Operativo è embedded , o è inaccessibile agli utilizzatori? .3						X	
A1.1	E' possibile bloccare l'uso delle porte USB libere? .4	se "NO" specificare il motivo					X	X
A1.1	Il software applicativo potrebbe essere installato su un computer / server di proprietà dell'Ospedale? .5	se "SI" specificare requisiti hw					X	
A1.2 Connettività di rete							X	
A1.2	L'apparecchiatura si connette alla rete aziendale? .1	se "SI" specificare LAN o WIFI					X	
A1.2	(se LAN) Numero prese di rete richieste (se WIFI) Frequenze supportate (GHz) .2						X	
A1.2	Necessita di accesso verso l'esterno per navigazione Internet? .3	se "SI" specificare quali protocolli: http, https, ftp, ...					X	X
A1.2	Necessita di accesso remoto dall'esterno per attività di manutenzione / aggiornamento? .4 (NB modalità accettate: VPN Lan-To-Lan, o Client-To-Lan by Cisco AnyConnect)						X	
A1.2	Il controllo da remoto si attiva solo dopo <u>esplicito consenso</u> dell'utilizzatore? .5						X	
A1.2	Invia <u>dati tecnici</u> , o <u>dati statistici di utilizzo</u> all'esterno? (per debugging, monitoraggio pro-attivo, statistiche d'uso, ...) .6	se "SI" specificare <u>quali dati</u> e <u>per quali scopi</u>					X	
A1.2	Utilizza connessioni Internet proprie (tramite SIM, modem, ecc)? .7	se "SI" specificare					X	
A1.3 Aggiornamento / protezione del Sistema Operativo e protezione Antivirus							X	
A1.3	(se Windows o OSX) E' possibile mantenere aggiornato il Sistema Operativo tramite servizi di dominio aziendale (configurabili tramite Microsoft SCCM o Apple AirWatch) ? .1						X	
A1.3	(se Windows) E' possibile installare un Antivirus aziendale? .2						X	
A1.3	Esistono dei percorsi da escludere dall'Antivirus? In quali cartelle sono installati gli eseguibili dell'Applicativo e del Database? .3	se "SI" specificare					X	
A1.3	(se Windows o OSX) Quali modalità di aggiornamento / quali policy di protezione e inviolabilità del Sistema Operativo vengono garantite dal Fornitore o Produttore? .4						X	
A2 GESTIONE ACCESSI AL SISTEMA							X	X
A2.1 Ambiente di utilizzo								
A2.1	Ambiente di utilizzo dell'apparecchiatura, indicare: .1 - <u>alta affluenza</u> di pz/operatori (es. ambulatori e simili) - <u>accesso ristretto</u> a pz/operatori selezionati (es. diagnostiche) - <u>accesso controllato</u> da badge o sistemi simili							X
A2.1	E' utilizzata per urgenze (h24)? .2							X
A2.2 Credenziali di accesso								

A2.2 .1	L'accesso all'Applicativo (o al Sistema Operativo) è protetto da credenziali o password? <i>(per ogni apparato IT)</i>				X	
A2.2 .2	Le credenziali sono autenticabili in dominio di rete aziendale (tramite <u>LDAPS</u> / Active Directory 2012 R2 / 2016)?				X	
A3 TRATTAMENTO E PROTEZIONE DEI DATI					X	X
A3.1 Dati prodotti						
A3.1 .1	Descrivere quali dati produce l'apparecchiatura <i>Immagini, tracciati, altri dati...</i>				X	X
A3.1 .2	Sono dati sensibili, riferiti o riferibili a persone fisiche? <i>(NB: dati che identificano il paziente tramite un codice sono considerati dati sensibili)</i>	se "SI" specificare se usato codice di pseudonimizzazione			X	X
A3.1 .3	In quale formato vengono esportati i dati?				X	
A3.2 Invio / accesso / ricezione dati entro la rete aziendale						X
A3.2 .1	Descrivere il flusso dei dati entro la rete aziendale <i>Indicare a quali computer / apparecchiature / applicativi / database, l'apparecchiatura si deve connettere ai fini di: invio / consultazione / elaborazione dei dati prodotti</i>					X
A3.2 .2	L'apparecchiatura si deve connettere con altri applicativi / apparecchiature in rete aziendale per ricevere dati in ingresso?	se "SI" specificare				X
A3.2 .3	I dati prodotti devono essere conservati su risorse di rete aziendali (backup aziendale)? <i>(NB: nessun dato conservato sull'apparecchiatura, o su hard disk portatili, o su flash drive, può essere ritenuto sicuro e recuperabile in caso di guasti, né rispondente ai requisiti di sicurezza e privacy, imposti dal GDPR 2016/679)</i>					X
A3.2 .4	Indicare nel dettaglio: - a che scopo (legale / pubblicazioni / archivio storico / ...); - spazio necessario (in GB o TB) per 1 anno di attività; - per quanti anni è necessario mantenere i dati in archivio.					X
A3.3 Invio / accesso dati all'esterno della rete aziendale					X	X
A3.3 .1	I dati devono essere inviati ad altri applicativi / database (o devono essere accessibili da altri applicativi) situati fuori dalla rete aziendale?	se "SI" specificare			X	X
A3.3 .2	Descrivere nel dettaglio: - in quale Paese è situato l'applicativo / database? - chi è il proprietario / da chi è gestito? - chi può accedere ai dati? - per quali finalità vengono trattati i dati?				X	X
A3.3 .3	L'applicativo / Il database può essere trasferito su un server virtualizzato aziendale?				X	