AMENDMENT 1	EMENDAMENTO N. 1
to the STANDARD CONTRACTUAL CLAUSES MASTER AGREEMENT	**al CLAUSOLE CONTRATTUALI TIPO ACCORDO QUADRO**
This Amendment 1 (hereinafter called the "Amendment") to the Standard Contractual Clauses Master Agreement ("Agreement") signed on the 13th of April 2023 shall enter into effect on the date of last signature below (the "Effective Date")	Il presente Emendamento n. 1 (di seguito denominato "Emendamento") all'Accordo quadro corredato di clausole contrattuali tipo ("Contratto") firmato il 13 aprile 2023 entrerà in vigore alla data dell'ultima firma qui sotto (la "Data di entrata in vigore")
and is made by and between:	è stipulato da e tra:
Janssen Research & Development, LLC, a United States corporation with registered office at 920 US Route 202 South, Raritan, NJ 08869-0602 (USA) (hereinafter "**Janssen**")	Janssen Research & Development, LLC, una società di diritto statunitense con sede legale in US Route 202 South n. 920, Raritan, NJ 08869-0602 (Stati Uniti) (di seguito denominata "**Janssen**")
and	e
Azienda Ospedaliero-Universitaria di Cagliari ("**Institution**"), with registered offices located at Via Ospedale 54, 09124 Cagliari, Italy	Azienda Ospedaliero-Universitaria di Cagliari ("**Istituto**"), con sede legale presso Via Ospedale 54, 09124 Cagliari, Italy
Hereinafter "the Parties"	di seguito congiuntamente "le Parti"
Whereas, the Parties have executed the Agreement on the 13th of April 2023.	**Premesso che,** le Parti hanno perfezionato il Contratto in data 13 aprile 2023
Whereas, the Parties wish to include an Annex to the Agreement that contains the Supplier Information Security Requirements ("SISR") to further explains the security measures taken by Janssen in the Clinical Studies.	**Premesso che,** le Parti desiderano includere un allegato al Contratto contenente i Requisiti di Sicurezza delle Informazioni del Fornitore ("SISR") per spiegare ulteriormente le misure di sicurezza adottate da Janssen negli Studi Clinici.
NOW THEREFOR, IN CONSIDERATIONS OF THE MUTUAL COVENANTS SET FORTH HEREIN, THE PARTIES AGREE AS FOLLOWS:	**TUTTO CIO' PREMESSO, TRA LE PARTI SI CONVIENE QUANTO SEGUE:**
ART. 1 **General Provisions**	**ART. 1** **(Previsioni generali)**
The Premises to the Agreement must be understood as integrated with those referred to in this Amendment, to be considered an integral and essential part of this Amendment and of the Agreement. The conditions and terms, as well as the obligations of the Parties, arising from the provisions of the Contract, which are not modified by this Amendment, remain unchanged.	Le Premesse al Contratto devono intendersi integrate da quelle di cui al presente Emendamento, da considerarsi parte integrante ed essenziale del presente Emendamento e del Contratto. Le condizioni ed i termini, nonché gli obblighi a carico delle Parti, nascenti dalle previsioni del Contratto, che non siano modificate dal presente Emendamento, rimangono invariati.
ARTICLE 2	**Art. 2**

(Modifications to contractual clauses)	(Modifiche alle clausole contrattuali)
Annex I to this Amendment should be added to the Agreement as Exhibit 2 I: Supplier Information Security Requirements ("SISR")	L'allegato I del presente Emendamento deve essere aggiunto al Contratto come Allegato II: Requisiti di sicurezza delle informazioni dei fornitori ("SISR")
Art. 3 **(Duration)**	**Art. 3** **(Validità)**
This Amendment comes into effect from the date of its last subscription.	Il presente Emendamento n. 1 entra in vigore a partire dalla data della sua ultima sottoscrizione.
All other contract clauses remain unchanged	Tutte le altre previsioni contrattuali rimangono invariate.
This Contract Amendment is signed digitally in accordance with Article 24 of legislative decree 82/2005, in accordance with the provisions of Article 15 paragraph 2A of Law 241/1990 as supplemented by article 6, decree law 18/10/2012, no. 179, converted into Law no. 22 of 17/12/2012. All the taxes and duties relating to or resulting from the stipulation of this Agreement, including the revenue stamp on the digital original as referred to in Article 2 of the table in Annex A – tariff part I of Presidential Decree 642/1972, and the registration tax, must be paid in accordance with the applicable regulations. The stamp duty on the digital text is borne by Janssen and is virtually paid by Janssen (Authorization of the Revenue Agency No. 1 of 5/3/2007 - Monza Office)	Il presente Emendamento viene sottoscritto con firma digitale ai sensi dell'art. 24 del D. Lgs. 82/2005, giusta la previsione di cui all'art. 15, comma 2bis della Legge n. 241/1990, come aggiunto dall'art. 6, D.L. 18/10/2012, n. 179, convertito in Legge 17/12/2012 n. 22. Le imposte e tasse inerenti e conseguenti alla stipula della presente seconda modifica, ivi comprese l'imposta di bollo sull'originale informatico di cui all'art. 2 della Tabella Allegato A – tariffa parte I del DPR n. 642/1972 e l'imposta di registro devono essere versate, nel rispetto della normativa applicabile. L'imposta di bollo sull'originale informatico, è a carico di Janssen ed è assolta virtualmente da Janssen (Autorizzazione Agenzia delle Entrate n. 1 del 5/3/2007 - Uff. Monza)
Read, confirmed, signed/digitally signed	Letto, confermato, sottoscritto/sottoscritto digitalmente
Janssen Research & Development, LLC	**Janssen Research & Development, LLC**
Signature_____ Date_____	Firma_____ Data_____
Represented by: Linda Tedder Global Site Contracting Resource Center Contracts/Grant GRO	Rappresentata da: Linda Tedder Global Site Contracting Resource Center Contracts/Grant GRO
Azienda Ospedaliero-Universitaria di Cagliari	**Azienda Ospedaliero-Universitaria di Cagliari**

Signature_____ Date_____	Firma_____ Data_____
Represented by: Dr. Chiara Seazzu Director	Rappresentata da: Dott.ssa Chiara Seazzu Director

List of Annexes:

Annex 1: Exhibit 2: Supplier Information Security Requirements ("SISR")

Elenco degli Allegati:

Allegato 1: Requisiti di sicurezza delle informazioni dei fornitori ("SISR")

Annex 1: Exhibit 2: Supplier Information Security Requirements ("SISR")	Allegato 1 Documento 2: Requisiti sulla sicurezza delle informazioni dei fornitori ("SISR")
This document specifies information security requirements applicable to Suppliers that provide goods or services to Johnson & Johnson and/or Johnson & Johnson Affiliates when Supplier will access, process, or store Johnson & Johnson Information. These information security requirements are consistent with the International Organization for Standardization (ISO) 27001/27002 Standards for Information Security Management Systems (ISMS).	Il presente documento specifica i requisiti di sicurezza delle informazioni applicabili ai Fornitori che forniscono beni o servizi a Johnson & Johnson e/o alle Affiliate Johnson & Johnson quando il Fornitore accederà, tratterà o archivierà le Informazioni di Johnson & Johnson. Questi requisiti di sicurezza delle informazioni sono coerenti con le norme previste per i sistemi di gestione della sicurezza delle informazioni (ISMS) dell'Organizzazione internazionale per la normazione (ISO) 27001/27002.
DEFINITIONS	**DEFINIZIONI**
The definitions below contain a series of terms that are used throughout this document. When encountering one of these capitalized terms, refer to the definition below.	Le seguenti definizioni contengono una serie di termini utilizzati in tutto il presente documento. Quando si incontra uno di questi termini in maiuscolo, fare riferimento alla definizione riportata di seguito.
Computing and Network Resources: All Systems, In-Scope Applications, Network Devices and Services, Facilities, Other Services, and Telecommunications resources, including those that are virtual or cloud-based, required to process, store, or transmit information.	**Risorse informatiche e di rete:** tutti i sistemi, le applicazioni nell'ambito, i dispositivi e i servizi di rete, le strutture, gli altri servizi e le risorse di telecomunicazione, compresi quelli virtuali o basati sul cloud, necessari per elaborare, archiviare o trasmettere informazioni.
Globally Recognized Standards: A standard or framework that has been generally accepted globally as superior to. The ISO 27000 Information Security Management System series is one example.	**Norme riconosciute a livello globale:** una norma o una struttura che è stata generalmente accettata come superiore a livello globale. La serie del Sistema di gestione della sicurezza informatica ISO 27000 ne è un esempio.
Globally Recognized Best Practice: A method or technique that has been generally accepted globally as superior to alternatives because it	**Best Practice riconosciuta a livello globale:** un metodo o una tecnica che è stata generalmente accettata a livello globale come superiore alle

achieves results that are superior to those achieved by other means	alternative, in quanto raggiunge risultati superiori a quelli ottenuti con altri mezzi
In-Scope Applications: Applications, including databases and Internet-facing websites, that store, transmit, or process Johnson & Johnson Information.	**Applicazioni nell'ambito:** applicazioni, compresi database e siti web rivolti a Internet, che archiviano, trasmettono o trattano le Informazioni di Johnson & Johnson.
ISO: The International Organization for Standardization is an independent, non-governmental organization, the members of which are the standards organizations of the 164 member countries. It is the world's largest developer of voluntary international standards and it facilitates world trade by providing common standards among nations. The ISO 27000 series on Information Security Management Systems is a de facto corporate information security standard for a large percentage of organizations worldwide.	**ISO:** l'Organizzazione internazionale per la normazione è un'organizzazione indipendente non governativa, i cui membri sono le organizzazioni per la normazione dei 164 Paesi membri. È il più grande sviluppatore al mondo di norme internazionali volontarie e facilita il commercio mondiale fornendo norme comuni tra le nazioni. La serie ISO 27000 sui sistemi di gestione della sicurezza informatica è una norma di sicurezza delle informazioni aziendali di fatto per una grande percentuale di organizzazioni in tutto il mondo.
Johnson & Johnson: All entities encompassing the entirety of Johnson & Johnson, worldwide, including Johnson & Johnson Affiliates.	**Johnson & Johnson:** tutte le entità che comprendono la totalità di Johnson & Johnson, in tutto il mondo, comprese le affiliate di Johnson & Johnson.
Johnson & Johnson Affiliate: Any entity that controls, is controlled by or under common control with Johnson & Johnson.	**Affiliata Johnson & Johnson:** qualsiasi entità che controlli, sia controllata da o sia sotto il controllo comune di Johnson & Johnson.
Johnson & Johnson Information: All data or information provided to Supplier by Johnson & Johnson that is necessary to deliver the services in this agreement, or any information generated by Supplier on behalf of Johnson & Johnson.	**Informazioni di Johnson & Johnson :** tutti i dati o le informazioni forniti al Fornitore da Johnson & Johnson che sono necessari per fornire i servizi previsti nel presente contratto o qualsiasi informazione generata dal Fornitore per conto di Johnson & Johnson.
Mobile Computing Device: Handheld personal computing devices that can store information and communicate over wireless networks (including cellular and/or Wi-Fi), such as smart phones, tablets, and PDAs.	**Dispositivo informatico mobile:** dispositivi di elaborazione personale portatili che possono archiviare informazioni e comunicare su reti wireless (compresi cellulare e/o Wi-Fi), come smartphone, tablet e PDA.
NIST: The National Institute of Standards and Technology, a standards body within the United States that produces, among other things, information technology and information security technical standards on a wide array of topics like cryptography. NIST standards are known globally.	**NIST:** National Institute of Standards and Technology, un organismo di normazione all'interno degli Stati Uniti che produce, tra le altre cose, tecnologie informatiche e standard tecnici per la sicurezza delle informazioni su una vasta gamma di argomenti come la crittografia. Le norme NIST sono note a livello globale.

Network Devices: Systems and appliances that are part of the network infrastructure, such as routers, switches, firewalls, caching and proxy servers, and load balancers.	**Dispositivi di rete:** sistemi e apparecchi che fanno parte dell'infrastruttura di rete, come router, switch, firewall, server di memorizzazione nella cache e proxy e bilanciatori di carico.
OWASP: The Open Web Application Security Project is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.	**OWASP:** Open Web Application Security Project è una comunità online che produce articoli, metodologie, documenti, strumenti e tecnologie liberamente disponibili nel campo della sicurezza delle applicazioni web.
Removable Storage Device: Any portable or removable device that stores electronic information and can be easily removed and transported (e.g., portable hard drive, memory stick, memory card, CD, DVD, back-up tape or device, etc.).	**Dispositivo di archiviazione rimovibile:** qualsiasi dispositivo portatile o rimovibile che memorizzi informazioni elettroniche e che possa essere facilmente rimosso e trasportato (per es. disco rigido portatile, memory stick, scheda di memoria, CD, DVD, nastro o dispositivo di backup, ecc.).
Server Systems: Shared computer systems, including servers that provide file and print, collaboration, groupware, instant messaging, file or data transfer, application, or email services.	**Sistemi server:** sistemi informatici condivisi, compresi i server che forniscono servizi di trasferimento di file e stampa, collaborazione, groupware, messaggistica istantanea, file o dati, applicazioni o e-mail.
Systems: User Systems and Server Systems.	**Sistemi:** sistemi utente e sistemi server.
User Systems: Personal computing devices used by an end-user, including desktops, laptops, workstations, and Mobile Computing Devices.	**Sistemi utente:** dispositivi informatici personali utilizzati da un utente finale, compresi desktop, portatili, workstation e dispositivi informatici mobili.
1 INFORMATION SECURITY POLICY	**1 POLITICA SULLA SICUREZZA DELLE INFORMAZIONI**
1.1 Supplier shall have a documented information security management system (ISMS) that aligns with a globally recognized standard such as ISO 27001 or the NIST CyberSecurity Framework. Supplier ISMS must include policies and procedures to ensure the confidentiality, integrity, and availability of Supplier and Johnson & Johnson Information.	1.1 Il Fornitore deve disporre di un Sistema di gestione della sicurezza informatica (ISMS) in linea con una norma riconosciuta a livello globale come ISO 27001 o NIST CyberSecurity Framework. L'ISMS del fornitore deve includere politiche e procedure volte a garantire la riservatezza, l'integrità e la disponibilità delle informazioni del fornitore e di Johnson & Johnson.
1.2 Supplier shall review and update, as necessary, its ISMS at least annually to ensure	1.2 Il Fornitore esaminerà e aggiornerà, se necessario, il proprio ISMS almeno una volta

the policies address current threats and remain consistent with the standards upon which it is built.	all'anno per garantire che le politiche affrontino le minacce attuali e rimangano coerenti con le norme su cui si basa.
2 INFORMATION SECURITY ORGANIZATION	**2 ORGANIZZAZIONE PER LA SICUREZZA DELLE INFORMAZIONI**
2.1 Supplier shall designate an individual responsible for information security within its organization (the "Information Security Officer") and have defined information security roles and responsibilities throughout the organization. Supplier shall provide the name and contact information of its designated Information Security Officer upon request.	2.1 Il Fornitore dovrà designare una persona responsabile della sicurezza delle informazioni all'interno della propria organizzazione (il "Responsabile della sicurezza delle informazioni") e avere ruoli e responsabilità definiti per la sicurezza delle informazioni in tutta l'organizzazione. Su richiesta, il Fornitore dovrà fornire il nome e le informazioni di contatto del proprio Responsabile della sicurezza delle informazioni designato.
3 SUPPLIER RELATIONSHIPS	**3 TIPI DI RAPPORTO CON I FORNITORI**
3.1 Supplier shall ensure non-disclosure or confidentiality agreements are in place with any contractor, subcontractor, and other related parties who have access to Supplier's internal networks and/or will store, process or transmit Johnson & Johnson Information.	3.1 Il Fornitore dovrà garantire che siano in essere accordi di non divulgazione o riservatezza con qualsiasi appaltatore, subappaltatore e altre parti correlate che abbiano accesso alle reti interne del Fornitore e/o archivieranno, tratteranno o trasmetteranno Informazioni di Johnson & Johnson.
3.2 Supplier shall maintain a documented third party risk management program based upon globally recognized industry security standards and conduct assessments of contractors, subcontractors and other related parties accordingly, and prior to sharing any Johnson & Johnson Information, establishing a network-to-network connection between their network and Supplier's internal network, or hosting a website or web application containing Johnson & Johnson Information.	3.2 Il Fornitore dovrà mantenere un programma documentato di gestione dei rischi di terze parti basato su norme di sicurezza del settore riconosciute a livello globale e condurre valutazioni di appaltatori, subappaltatori e altre parti correlate di conseguenza e, prima di condividere qualsiasi informazione di Johnson & Johnson, stabilendo una connessione rete-rete tra la propria rete e la rete interna del Fornitore oppure ospitando un sito web o un'applicazione web contenente Informazioni di Johnson & Johnson.

3.3 Supplier shall be responsible for ensuring that security requirements consistent with these Johnson & Johnson Supplier Information Security Requirements, are included in contracts with, and are met by all Supplier contractors, subcontractors and other related parties who have access to, or will store, process or transmit Johnson & Johnson Information.	3.3 Il Fornitore avrà la responsabilità di garantire che i Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson, siano inclusi nei contratti con, e siano rispettati da tutti i terzisti, subappaltatori e altre parti correlate del Fornitore che hanno accesso a, o archivieranno, tratteranno o trasmetteranno le Informazioni di Johnson & Johnson.
4 ASSET MANAGEMENT	**4 GESTIONE DELLE RISORSE**
RESPONSIBILITY FOR ASSETS	**RESPONSABILITÀ PER LE RISORSE**
4.1 Supplier shall maintain an inventory of its hardware, software, and virtual assets that documents the identification, ownership, usage, location and configuration for each item.	4.1 Il Fornitore manterrà un inventario dei propri hardware, software e risorse virtuali che documenta l'identificazione, la proprietà, l'utilizzo, la posizione e la configurazione di ciascun elemento.
4.2 Supplier shall maintain documentation and other records of baseline system and security configurations, including configuration changes for all hardware, software, and virtual system components.	4.2 Il Fornitore dovrà conservare la documentazione e altri registri delle configurazioni del sistema di base e di sicurezza, comprese le modifiche alla configurazione di tutti i componenti hardware, software e del sistema virtuale.

4.3 Supplier shall have formal policies and practices for performing risk assessments of software, systems, networking and facilities. This includes classifying information and information systems, identifying security requirements, assessing and ensuring compliance with Supplier's policies and other applicable requirements, and adhering to change management processes.	4.3 Il Fornitore deve disporre di politiche e pratiche formali per eseguire valutazioni dei rischi di software, sistemi, reti e strutture. Ciò include la classificazione delle informazioni e dei sistemi informativi, l'identificazione dei requisiti di sicurezza, la valutazione e la verifica della conformità alle politiche del fornitore e ad altri requisiti applicabili e l'osservanza dei processi di gestione delle modifiche.
MEDIA HANDLING	**GESTIONE DEI MEDIA**
4.4 Where Johnson & Johnson specifies the requirement to encrypt Johnson & Johnson Information in storage, it shall be encrypted according to the requirements in Section 10, Cryptography.	4.4 Laddove Johnson & Johnson specifichi il requisito di crittografare le Informazioni di Johnson & Johnson in archivio, esse devono essere criptate in base ai requisiti della Sezione 10, Crittografia.
4.5 Discarding media (paper, film or electronic) containing any Johnson & Johnson Information shall be performed in accordance with NIST SP 800-88 Guidelines for Media Sanitization, or by a process approved by Johnson & Johnson.	4.5 L'operazione di scartare i media (cartacei, cinematografici o elettronici) contenenti qualsiasi informazione di Johnson & Johnson deve essere eseguita in conformità con le linee guida NIST SP 800-88 riguardanti le Procedure di sanitizzazione dei supporti o mediante un processo approvato da Johnson & Johnson.
5 HUMAN RESOURCES SECURITY	**5 SICUREZZA DELLE RISORSE UMANE**
5.1 Supplier shall ensure that its employees, contractors, and other users understand their responsibilities regarding information security through initial and periodic refresher information security training that includes:	5.1 Il Fornitore dovrà garantire che i propri dipendenti, appaltatori e altri utenti comprendano le proprie responsabilità in materia di sicurezza delle informazioni attraverso una formazione iniziale e periodica di aggiornamento sulla sicurezza delle informazioni che includano:
• Proper selection of passwords and PINs, and how to keep them private.	• Una corretta selezione di password e PIN e come mantenerli privati.
• Responsible use of computing resources: never leave an unlocked device unattended, maintain control of devices in public, secure portable storage, etc.	• Uso responsabile delle risorse informatiche: non lasciare mai un dispositivo sbloccato incustodito, mantenere il controllo dei dispositivi in pubblico, garantire conservazione portatili, ecc.
• Simulated Phishing attacks or other situational awareness mechanisms.	• Simulazione di attacchi di phishing o di altri meccanismi di consapevolezza situazionale.

• Reminders that paper documents also need to be protected properly.	• Promemoria che anche i documenti cartacei devono essere protetti correttamente.
5.2 Supplier shall conduct background checks and/or other investigations deemed necessary, as appropriate and permitted by applicable law, on all individuals. Supplier shall perform additional investigations in accordance with the identified criticality and sensitivity of the position and information the individual may have access to, as permitted by applicable law.	5.2 Il Fornitore dovrà condurre controlli dei precedenti personali e/o altre indagini ritenute necessarie, come appropriato e consentito dalla legge vigente, su tutti i soggetti. Il Fornitore dovrà eseguire ulteriori indagini in conformità con la criticità e la sensibilità identificate della posizione e le informazioni a cui il soggetto può avere accesso, così come consentito dalla legge vigente.
5.3 Supplier shall ensure that its administrators are adequately trained on the Computing and Network Resources for which they are responsible, and training records are maintained.	5.3 Il Fornitore dovrà garantire che i propri amministratori siano adeguatamente formati sulle Risorse informatiche e di rete di cui sono responsabili e che vengano conservati i registri di formazione.
5.4 Supplier shall have a disciplinary process in place for policy violations.	5.4 Il Fornitore deve disporre di un processo disciplinare per le violazioni della politica.
5.5 Supplier shall promptly terminate personnel access to Supplier's Computing and Network Resources and facilities and other secure areas when an individual leaves or discontinues work for Supplier, or no longer needs access.	5.5 Il Fornitore dovrà interrompere prontamente l'accesso del personale alle Risorse informatiche e di rete, alle strutture del Fornitore e ad altre aree sicure quando un soggetto lascia o interrompe il lavoro per il Fornitore o non ha più bisogno di accedervi.
5.6 Supplier shall have formal policies in place to ensure that its employees, contractors and other users abide by acceptable use of Computing and Network Resources for ethical, lawful, and productive use of those resources, and to avoid prohibited use and actions.	5.6 Il Fornitore deve disporre di politiche formali volte a garantire che i propri dipendenti, appaltatori e altri utenti rispettino un uso accettabile delle Risorse informatiche e di rete per un uso etico, legale e produttivo di tali risorse e a evitare un uso e azioni vietati.
6 PHYSICAL AND ENVIRONMENTAL SECURITY OF SECURE AREAS	**6 SICUREZZA FISICA E AMBIENTALE DELLE AREE SICURE**
6.1 Supplier shall implement physical access control mechanisms (e.g., electronic access control, locks) to ensure only authorized individuals can obtain physical access to Supplier facilities.	6.1 Il Fornitore deve implementare meccanismi di controllo dell'accesso fisico (per es. controllo dell'accesso elettronico, chiusure) per garantire che solo i soggetti autorizzati possano ottenere l'accesso fisico alle strutture del Fornitore.
6.2 Supplier shall lock and/or have strong access controls in place to control access to all of its	6.2 Il Fornitore dovrà bloccare e/o disporre di controlli di accesso validi per controllare

data centers, equipment rooms, telecommunication closets and utilities.	l'accesso a tutti i suoi data center, locali delle apparecchiature, armadi per le telecomunicazioni e servizi.
6.3 Supplier shall control unauthorized access to unattended areas (e.g., offices, conference rooms, etc.) within a Supplier facility that contains Johnson & Johnson Information by using locks or equivalent means.	6.3 Il Fornitore dovrà controllare l'accesso non autorizzato alle aree incustodite (per es. uffici, sale conferenze, ecc.) all'interno di una struttura del Fornitore che contenga Informazioni di Johnson & Johnson ricorrendo a serrature o mezzi equivalenti.
6.4 Supplier shall conduct regular but no less than annual inspections of the perimeter and all access control mechanisms to provide assurance that its hardware cannot be easily manipulated or bypassed to gain unauthorized access.	6.4 Il Fornitore dovrà condurre ispezioni regolari ma non meno che annuali del perimetro e di tutti i meccanismi di controllo dell'accesso per garantire che il suo hardware non possa essere manipolato o bypassato facilmente per ottenere un accesso non autorizzato.
6.5 Supplier shall ensure facilities and data centers are resilient to natural or man-made disasters. Supplier shall ensure that its personnel within Supplier's facilities (e.g., employees, visitors, resident contractors) are able to be immediately identified (e.g., using identification badges, visual recognition or other means).	6.5 Il Fornitore dovrà garantire che le strutture e i data center siano in grado di resistere a disastri naturali o causati dall'uomo. Il Fornitore dovrà garantire che il suo personale all'interno delle strutture del Fornitore (per es. dipendenti, visitatori, appaltatori residenti) possa essere immediatamente identificato (per es. utilizzando badge identificativi, riconoscimento visivo o altri mezzi).
6.6 Supplier facilities that contain Server Systems or In-Scope Applications that store, process or transmit Johnson & Johnson Information shall have all data center access/egress points monitored by security staff and/or recorded with security cameras twenty-four (24) hours a day, seven (7) days a week. Security camera recordings shall be stored for no less than ninety (90) days or according to local law.	6.6 Le strutture del fornitore che contengono sistemi server o applicazioni nell'ambito che archiviano, elaborano o trasmettono Informazioni di Johnson & Johnson devono avere tutti i punti di accesso/uscita del data center monitorati dal personale di sicurezza e/o registrati con le videocamere di sicurezza ventiquattro (24) ore al giorno, sette (7) giorni alla settimana. Le registrazioni delle videocamere di sicurezza devono essere conservate per non meno di novanta (90) giorni o in conformità alla legge locale.
6.7 Supplier shall secure Johnson & Johnson Information in paper form when not in use.	6.7 Il Fornitore dovrà proteggere le Informazioni di Johnson & Johnson redatte in forma cartacea quando non vengono utilizzate.
6.8 Supplier shall always escort visitors where Johnson & Johnson Information or access to Supplier internal networks is readily accessible. Supplier data centers shall have a unique registry for all visitors and maintain access control logs.	6.8 Il Fornitore accompagnerà sempre i visitatori ai quali le Informazioni di Johnson & Johnson o l'accesso alle reti interne del Fornitore sono facilmente accessibili. I data center dei fornitori devono disporre di un registro univoco per tutti i visitatori e mantenere i registri di controllo degli accessi.

6.9 Supplier shall control delivery and loading areas and isolate these areas and storage areas from data centers, if possible, to avoid unauthorized access.	6.9 Il Fornitore deve controllare le aree di consegna e caricamento e isolare queste aree e le aree di stoccaggio dai data center, se possibile, per evitare l'accesso non autorizzato.
6.10 Supplier shall protect Systems, Network Devices and other equipment to reduce the risk from environmental threats and hazards and opportunities for unauthorized access.	6.10 Il Fornitore dovrà proteggere i Sistemi, i Dispositivi di rete e altre apparecchiature per ridurre il rischio di minacce ambientali, pericoli e opportunità di accesso non autorizzato.
6.11 Supplier shall ensure that all Systems, Network Devices and other equipment used to process or store Johnson & Johnson Information are protected from theft, loss and unauthorized access.	6.11 Il Fornitore dovrà garantire che tutti i Sistemi, i Dispositivi di rete e altre apparecchiature utilizzati per elaborare o archiviare le Informazioni di Johnson & Johnson siano protetti da furto, perdita e accesso non autorizzato.
6.12 Supplier shall protect power-dependent equipment from power failures, surges and other electrical anomalies.	6.12 Il Fornitore dovrà proteggere le apparecchiature dipendenti dall'alimentazione da interruzioni di alimentazione, sovratensioni e altre anomalie elettriche.
6.13 Supplier shall ensure that all power, telecommunication and network cabling is protected from unauthorized access and damage.	6.13 Il Fornitore dovrà garantire che tutti i cavi di alimentazione, telecomunicazioni e rete siano protetti da accessi non autorizzati e da danni.
6.14 Supplier shall have appropriate procedures in place to control unauthorized removal of Server Systems and Network Devices.	6.14 Il Fornitore deve disporre di procedure appropriate per controllare la rimozione non autorizzata dei Sistemi server e dei Dispositivi di rete.
6.15 Supplier shall check all Systems and Network Devices that may have contained Johnson & Johnson Information to ensure that all such information has been securely removed prior to redeployment or disposal.	6.15 Il Fornitore controllerà tutti i Sistemi e i Dispositivi di rete che potrebbero aver contenuto le Informazioni di Johnson & Johnson per garantire che tali informazioni siano state rimosse in modo sicuro prima della ridistribuzione o dello smaltimento.
7 OPERATIONS SECURITY	**7 SICUREZZA DELLE OPERAZIONI**
OPERATIONAL PROCEDURES AND RESPONSIBILITIES	**PROCEDURE OPERATIVE E RESPONSABILITÀ**
7.1 Supplier shall have standard operating procedures and supporting work instructions in place for operational management of Supplier's Computing and Network Resources.	7.1 Il Fornitore deve disporre di procedure operative standard e di istruzioni di lavoro di supporto per la gestione operativa delle Risorse informatiche e di rete del Fornitore.

7.2 Supplier shall have a documented change management process and supporting governance in place to control all changes to Computing and Network Resources.	7.2 Il Fornitore deve disporre di un processo documentato di gestione delle modifiche e di governance di supporto per controllare tutte le modifiche apportate alle Risorse informatiche e di rete.
7.3 Supplier shall segregate duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of Supplier's assets. The segregation of duties shall be documented.	7.3 Il Fornitore dovrà separare i doveri e le aree di responsabilità per ridurre le opportunità di modifica non autorizzata o non intenzionale o di uso improprio dei beni del Fornitore. La separazione dei compiti deve essere documentata.
7.4 Supplier shall separate development, test and operational/production environments to reduce the risks of unauthorized access or changes to the operational system or information.	7.4 Il Fornitore dovrà separare gli ambienti di sviluppo, test e operativi/produzione per ridurre i rischi di accesso non autorizzato o di modifiche al sistema operativo o alle informazioni.
SYSTEM PLANNING AND ACCEPTANCE	**PIANIFICAZIONE E ACCETTAZIONE DEL SISTEMA**
7.5 Supplier shall establish acceptance criteria for new Systems and Network Devices during development and prior to production release.	7.5 Il Fornitore deve stabilire i criteri di accettazione per i nuovi Sistemi e Dispositivi di rete durante lo sviluppo e prima del rilascio della produzione.
7.6 Supplier shall complete Security Configuration Standards or "hardening documents" for all Server Systems, In-Scope Applications and Network Devices prior to placing them in production to ensure compliance with these Johnson & Johnson Supplier Information Security Requirements and industry best practices.	7.6 Il Fornitore dovrà completare le Norme di configurazione della sicurezza o i "documenti configurati per la sicurezza" di tutti i Sistemi server, le Applicazioni nell'ambito e i Dispositivi di rete prima di metterli in produzione, per garantire la conformità ai presenti Requisiti sulla sicurezza delle informazioni dei fornitori Johnson & Johnson e alle migliori pratiche del settore.
PROTECTION AGAINST MALICIOUS AND MOBILE CODE	**PROTEZIONE DA CODICE MOBILE DANNOSO**
Supplier shall implement the following malicious software and mobile code controls:	*Il Fornitore dovrà implementare i controlli dei seguenti software dannosi e del codice mobile:*
7.7 Anti-malware software where commercially available shall be installed, properly configured, and always running on User Systems and Server Systems. The software shall be configured to	7.7 Il software anti-malware, ove disponibile in commercio, deve essere installato, correttamente configurato e sempre in funzione sui Sistemi utente e sui Sistemi server. Il

protect against all known threats, including, but not limited to viruses, worms, Trojans, rootkits, spyware and keystroke loggers.	software deve essere configurato per proteggere da tutte le minacce note, tra cui, a titolo esemplificativo ma non esaustivo, virus, worm, trojan, rootkit, spyware e registratori di tasti.
7.8 A documented exception process must be followed for any system that will not have anti-malware running.	7.8 È necessario seguire un processo documentato di eccezione per qualsiasi sistema che non sarà dotato di un sistema antimalware.
7.9 Where the anti-malware software supports alerting, all malware detections shall be automatically and immediately reported to personnel directly responsible for the infected device, who shall address the alert and the root cause.	7.9 Laddove il software anti-malware supporti l'avviso, tutti i rilevamenti di malware devono essere segnalati automaticamente e immediatamente al personale direttamente responsabile del dispositivo infetto che deve gestire l'avviso e la causa principale.
7.10 Upon detection of malicious software or content, the malware shall be immediately quarantined, blocked, disabled, confiscated or otherwise halted to ensure it does not spread. Detection and evidence gathering shall comply with all applicable laws and government regulations.	7.10 Al momento del rilevamento di software o contenuti dannosi, il malware deve essere immediatamente messo in quarantena, bloccato, disabilitato, confiscato o altrimenti interrotto per garantire che non si diffonda. Il rilevamento e la raccolta delle prove devono essere conformi a tutte le leggi e alle normative governative applicabili.
7.11 Devices shall be scanned regularly in accordance with globally recognized best practices and standards (e.g., NIST Special Publication 800-83).	7.11 I dispositivi devono essere scansionati regolarmente in conformità con la migliore Best Practice e norme riconosciute a livello globale (per es. Pubblicazione speciale NIST 800-83).
7.12 Anti-malware software, including patches, version updates and engine updates shall be kept up to date.	7.12 Il software anti-malware, comprese le patch, gli aggiornamenti delle versioni e gli aggiornamenti del motore, deve essere mantenuto aggiornato.
7.13 Anti-malware signature definition files shall be updated within 72 hours of release by the vendor for all Systems.	7.13 I file di definizione della firma anti-malware devono essere aggiornati entro 72 ore dal rilascio da parte del fornitore per tutti i sistemi.
7.14 If Supplier performs code signing, Supplier shall have a documented code signing procedure that covers approval, private key protection and acceptable use.	7.14 Se il Fornitore esegue la firma del codice, il Fornitore deve disporre di una procedura documentata di firma del codice che copra l'approvazione, la protezione della chiave privata e l'uso accettabile.
BACKUP	**BACKUP**
7.15 Data and configuration backups shall be performed based on the business requirements	7.15 I backup di dati e configurazione devono essere eseguiti in base ai requisiti aziendali per

to maximize data availability and prevent Johnson & Johnson Information loss if the original data becomes unavailable.	massimizzare la disponibilità dei dati e prevenire la perdita di Informazioni di Johnson & Johnson se i dati originali non sono disponibili.
7.16 Data backup and recovery events shall be logged.	7.16 Gli eventi di backup e recupero dei dati devono essere registrati.
7.17 Data backups shall be performed immediately prior to any system upgrade or maintenance activity.	7.17 I backup dei dati devono essere eseguiti immediatamente prima di qualsiasi attività di aggiornamento o manutenzione del sistema.
7.18 Johnson & Johnson information that is required to be encrypted in storage by these Johnson & Johnson Supplier Information Security Requirements shall remain encrypted throughout the Data backup process.	7.18 Le Informazioni di Johnson & Johnson che devono essere crittografate nell'archiviazione da parte dei presenti Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson devono rimanere crittografate per tutta la durata del processo di backup dei dati.
7.19 Data backups shall be stored in a geographically separate, physically secure facility or cloud platform.	7.19 I backup dei dati devono essere archiviati in una struttura o piattaforma cloud geograficamente separata e fisicamente sicura.
7.20 Supplier shall test the ability to restore Data backups no less frequently than annually.	7.20 Il Fornitore dovrà testare la capacità di ripristinare i backup dei Dati con una frequenza non inferiore a quella annuale.
TECHNICAL VULNERABILITY MANAGEMENT	**GESTIONE DELLA VULNERABILITÀ TECNICA**
Supplier shall implement a vulnerability management program that follows globally recognized standards and includes the following controls:	*Il Fornitore deve implementare un programma di gestione delle vulnerabilità che segua le norme riconosciute a livello globale e includa i seguenti controlli:*
7.21 Application and system owners shall regularly monitor applicable sources for information regarding security bulletins or the release of security patches from vendors.	7.21 I proprietari di applicazioni e sistemi devono monitorare regolarmente le fonti applicabili per le informazioni relative ai bollettini di sicurezza o al rilascio di patch di sicurezza da parte dei fornitori.
7.22 Vendor-supplied security patches shall be analyzed and assigned a risk level. Critical patches shall be applied within 30 days of release by the vendor; all other patches shall be applied as soon as practical.	7.22 Le patch di sicurezza fornite dal fornitore devono essere analizzate e assegnate a un livello di rischio. Le patch importanti devono essere applicate entro 30 giorni dal rilascio da parte del fornitore; tutti le altre patch devono essere applicate non appena possibile.
7.23 Supplier shall use an industry standard vulnerability scanning tool to perform	7.23 Il Fornitore dovrà utilizzare uno strumento di scansione delle vulnerabilità standard del

vulnerability scans of pre-production Internet-facing Server Systems and Network Devices prior to moving those Server Systems/Network Devices to production. Vulnerabilities identified in pre-production testing shall be remediated prior to moving the Server System or Network Device to production.	settore per eseguire scansioni delle vulnerabilità dei Sistemi server e dei Dispositivi di rete rivolti a Internet di pre-produzione prima di trasferire tali Sistemi server/Dispositivi di rete alla produzione. Le vulnerabilità identificate nei test di pre-produzione devono essere risolte prima di spostare il Sistema server o il Dispositivo di rete alla produzione.
7.24 Supplier shall use an industry standard vulnerability scanning tool to perform vulnerability scans of all production Internet-facing Server Systems and Network Devices on a monthly basis. Critical vulnerabilities identified in production systems shall be remediated within 30 days of release by the vendor.	7.24 Il Fornitore utilizzerà uno strumento di scansione delle vulnerabilità standard del settore per eseguire scansioni delle vulnerabilità di tutti i Sistemi server e i Dispositivi di rete rivolti a Internet su base mensile. Le vulnerabilità critiche identificate nei sistemi di produzione devono essere risolte entro 30 giorni dal rilascio da parte del fornitore.
7.25 Supplier shall use an industry standard vulnerability scanning tool to perform a dynamic scan prior to the deployment of a new website/web application to Production, or prior to the deployment of major upgrades/customizations to an existing website/web application to Production. Scan must, at a minimum, look for the Open Web Application Security Project current top ten most common web applicable security risks ("OWASP Top 10"). Vulnerabilities identified in pre-production scanning shall be remediated prior to moving the application or website to production.	7.25 Il Fornitore dovrà utilizzare uno strumento di scansione delle vulnerabilità standard del settore per eseguire una scansione dinamica prima della distribuzione di un nuovo sito web/applicazione web alla Produzione o prima della distribuzione di upgrade/personalizzazioni principali a un sito web/applicazione web esistente alla Produzione. La scansione deve, come minimo, cercare gli attuali dieci rischi di sicurezza più comuni dell'Open Web Application Security Project applicabili al web ("OWASP Top 10"). Le vulnerabilità identificate nella scansione pre-produzione devono essere risolte prima di trasferire l'applicazione o il sito web alla produzione.
7.26 Supplier shall use an industry standard vulnerability scanning tool to perform dynamic scans of both production Internet-facing, web-based In-Scope Applications and production Internet-facing websites hosting Johnson & Johnson Information for, at a minimum, the OWASP Top 10 on a quarterly basis.	7.26 Il Fornitore dovrà utilizzare uno strumento di scansione delle vulnerabilità standard del settore per eseguire scansioni dinamiche delle applicazioni nell'ambito basate su Internet e dei siti Web di produzione basati su Internet che ospitano le Informazioni di Johnson & Johnson per almeno i Top 10 di OWASP su base trimestrale.
7.27 Vulnerabilities identified in production applications shall be analyzed and verified under the guidance of vendor recommendations and globally recognized standards like ISO or NIST. High risk or critical flaws shall be remediated within 60 days of identification; all others shall be remediated as soon as practical.	7.27 Le vulnerabilità identificate nelle applicazioni di produzione devono essere analizzate e verificate sotto la guida di raccomandazioni dei fornitori e delle norme riconosciute a livello globale come quelle ISO o NIST. I difetti ad alto rischio o critici devono essere corretti entro 60 giorni

	dall'identificazione; tutti gli altri devono essere risolti non appena possibile.
EXCHANGE OF INFORMATION	**SCAMBIO DI INFORMAZIONI**
7.28 Supplier shall have policies, procedures, and controls in place to protect the exchange of Johnson & Johnson Information through the use of all types of communication mechanisms.	7.28 Il Fornitore deve disporre di politiche, procedure e controlli per proteggere lo scambio di Informazioni di Johnson & Johnson mediante l'uso di tutti i tipi di meccanismi di comunicazione.
7.29 Supplier shall encrypt Johnson & Johnson Information in a manner compliant with Section 10, Cryptography, when transmitted electronically, including wirelessly, over any network other than the internal Supplier network.	7.29 Il Fornitore dovrà crittografare le Informazioni di Johnson & Johnson in modo conforme alla Sezione 10, Crittografia, quando trasmesse elettronicamente, anche in modalità wireless, su qualsiasi rete diversa dalla rete interna del Fornitore.
7.30 Supplier shall use reliable transport or couriers when transporting physical media containing Johnson & Johnson Information and use sufficient packaging to protect the content.	7.30 Il Fornitore dovrà utilizzare trasporti o corrieri affidabili per il trasporto di mezzi fisici contenenti Informazioni di Johnson & Johnson e utilizzare imballaggi sufficienti a proteggere il contenuto.
7.31 Supplier shall have policies and procedures in place to protect Johnson & Johnson Information associated with the interconnection of business information systems with any external entity.	7.31 Il Fornitore deve disporre di politiche e procedure per proteggere le Informazioni di Johnson & Johnson associate all'interconnessione di sistemi informativi aziendali con qualsiasi entità esterna.
LOGGING AND MONITORING	**REGISTRAZIONE E MONITORAGGIO**
7.32 Audit logging shall be enabled on Network Devices and Server Systems that contain Johnson & Johnson Information, In-Scope Applications and all security-related systems and appliances (e.g., identity and access management systems, domain controllers, anti-malware management servers, etc.), where supported by the log source system, to capture at a minimum the security-related events defined below:	7.32 La registrazione delle revisioni deve essere abilitata sui dispositivi di rete e sui sistemi server che contengono Informazioni di Johnson & Johnson, applicazioni nell'ambito e tutti i sistemi e gli apparecchi relativi alla sicurezza (per es. sistemi di gestione dell'identità e dell'accesso, controller di dominio, server di gestione anti-malware, ecc.), laddove supportati dal sistema di origine del registro, per acquisire almeno gli eventi relativi alla sicurezza definiti di seguito:
• Account logon (both successful and unsuccessful) and logoff	• Accesso account (sia riuscito sia non riuscito) e disconnessione
• Failed access attempts	• Tentativi di accesso non riusciti

• Account lockouts	• Lockout dell'account
• Elevation of privileges (both successful and unsuccessful), and every use of elevated privileges or actions taken while privilege is elevated	• Aumento dei privilegi (sia con successo sia senza) e ogni uso di privilegi o azioni elevate intraprese mentre il privilegio è elevato
• Creation, modification and deletion (both successful and unsuccessful) of:	• Creazione, modifica e cancellazione (sia riuscite sia non) di:
o Accounts or logon identifiers	o Account o identificativi di accesso
o Group membership	o Appartenenza al gruppo
o Access privileges/attributes for accounts and groups	o Privilegi/attributi di accesso per account e gruppi
o User rights and permissions	o Diritti e autorizzazioni dell'utente
• Changes in account or logon identifier status (both successful and unsuccessful)	• Modifiche allo stato dell'identificatore dell'account o dell'accesso (sia riuscite sia non)
• Modifications to, or unauthorized attempts to modify, the security configuration, security function or authorization policy	• Modifiche o tentativi non autorizzati di modificare la configurazione di sicurezza, la funzione di sicurezza o la politica di autorizzazione
7.33 Audit logs shall capture, at a minimum, the information for each security-related event defined below:	7.33 I registri delle revisioni devono acquisire, come minimo, le informazioni per ciascun evento relativo alla sicurezza definito di seguito:
• User, system or process identifier that triggered the event	• Identificatore dell'utente, del sistema o del processo che ha attivato l'evento
• Description of the event	• Descrizione dell'evento
• Date and time the event occurred (the date and time must be periodically synchronized to ensure it is accurate)	• Data e ora in cui si è verificato l'evento (la data e l'ora devono essere periodicamente sincronizzate per garantire che siano accurate)
• Identifier of the system generating the event (e.g., IP address)	• Identificatore del sistema che genera l'evento (per es. indirizzo IP)
• Authorization information associated with the event	• Informazioni di autorizzazione associate all'evento
7.34 Audit logs shall be retained for not less than ninety (90) days.	7.34 I registri delle revisioni devono essere conservati per non meno di novanta (90) giorni.
7.35 Audit logs and/or error reports shall be reviewed at least weekly for critical systems (domain controllers, remote access gateways, etc.) and at least monthly for all other systems,	7.35 I registri delle revisioni e/o i rapporti sugli errori devono essere esaminati almeno una volta alla settimana per i sistemi critici (controller di dominio, gateway di accesso remoto, ecc.) e almeno una volta al mese per

or in response to a security notification from an audit system.	tutti gli altri sistemi o in risposta a una notifica di sicurezza da parte di un sistema di revisione.
7.36 Audit logs shall be protected from accidental or intentional modification or destruction and Computing and Network Resources shall be automatically synchronized to a trusted time source.	7.36 I registri delle revisioni devono essere protetti da modifiche o distruzione accidentale o intenzionale e le Risorse informatiche e di rete devono essere sincronizzate automaticamente con una fonte di orario attendibile.
7.37 Applicable IDS/IPS events and alerts, and other security alerts/events generated by other Computing and Network Resources, shall be handled according to Supplier's security incident monitoring, reporting and response process.	7.37 Gli eventi e gli avvisi IDS/IPS applicabili e altri avvisi/eventi di sicurezza generati da altre Risorse informatiche e di rete devono essere gestiti in base al processo di monitoraggio, segnalazione e risposta degli incidenti di sicurezza del Fornitore.
MOBILE COMPUTING	**MOBILE COMPUTING**
Supplier shall implement the following mobile computing controls:	*Il Fornitore dovrà implementare i seguenti controlli di mobile computing:*
7.38 Supplier management approval must be obtained before User Systems may be used to store or transmit Johnson & Johnson Information.	7.38 Prima di poter utilizzare i Sistemi utente per archiviare o trasmettere le Informazioni di Johnson & Johnson è necessario ottenere l'approvazione della gestione dei fornitori.
7.39 User Systems shall be physically protected and require password authentication in accordance with Johnson & Johnson Supplier Information Security Requirements, which cannot be bypassed.	7.39 I Sistemi utente devono essere protetti fisicamente e richiedere l'autenticazione con password in conformità con i Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson che non possono essere bypassati.
7.40 Except as expressly set forth in these Johnson & Johnson Supplier Information Security Requirements, a Mobile Computing Device is treated no differently than any other User System.	7.40 Salvo quanto espressamente stabilito nei presenti Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson, un Dispositivo informatico mobile non è trattato in modo diverso da qualsiasi altro Sistema utente.
7.41 Mobile Computing Devices and any portable device containing Johnson & Johnson Information shall be encrypted at the device level (i.e., full disk encryption). This includes but is not limited to mobile phones, tablets, laptops, USB storage.	7.41 I dispositivi informatici mobili e qualsiasi dispositivo portatile contenente Informazioni di Johnson & Johnson devono essere crittografati a livello di dispositivo (ovvero crittografia completa del disco). Ciò include, a titolo esemplificativo ma non esaustivo, telefoni cellulari, tablet, portatili, dispositivi di memorizzazione USB.

7.42 Mobile Computing Devices containing Johnson & Johnson Information shall be configured to wipe information residing on the device (i.e., erasing the information or ensuring the encryption key protecting the information is erased) upon a remote command or after ten consecutive failed attempts to authenticate to the device. Remote wipe commands to erase Johnson & Johnson Information shall be sent when the device is lost or stolen or upon detection that the security controls have been circumvented.	7.42 I dispositivi mobili contenenti Informazioni di Johnson & Johnson devono essere configurati per cancellare le informazioni che risiedono sul dispositivo (ovvero cancellare le informazioni o garantire che la chiave di crittografia che protegge le informazioni sia cancellata) tramite un comando remoto o dopo dieci tentativi consecutivi di autenticazione del dispositivo. I comandi di cancellazione remota per cancellare le Informazioni di Johnson & Johnson devono essere inviati quando il dispositivo viene perso o rubato o quando viene rilevato che sono stati aggirati i controlli di sicurezza.
8 COMMUNICATIONS SECURITY	**8 SICUREZZA DELLE COMUNICAZIONI**
NETWORK SECURITY MANAGEMENT	**GESTIONE DELLA SICUREZZA DI RETE**
8.1 A firewall shall be in place to protect access to Supplier networks. Firewall(s) shall define and enforce rules over information and users crossing between internal and external systems.	8.1 Deve essere predisposto un firewall per proteggere l'accesso alle reti dei fornitori. Il/i firewall deve/devono definire e applicare regole sulle informazioni e sugli utenti che passano attraverso i sistemi interni ed esterni.
8.2 Firewall rules shall allow or deny connections over both outbound and inbound connections. Access which is not explicitly allowed shall be denied.	8.2 Le regole del firewall consentono o negano le connessioni sia in uscita sia in entrata. L'accesso non esplicitamente consentito deve essere negato.
8.3 All access allowed by the firewall, and all changes to the hardware, software or configuration of the firewall shall have a documented business purpose and an associated risk assessment and be approved by the Supplier's Information Security Officer or delegate.	8.3 Tutti gli accessi consentiti dal firewall e tutte le modifiche all'hardware, al software o alla configurazione del firewall devono avere uno scopo aziendale documentato e una valutazione dei rischi associata e devono essere approvati dal responsabile della sicurezza delle informazioni del fornitore o dal suo delegato.
8.4 Any direct or remote administrative session on a firewall shall not display the last user to log in and shall be logged off when unattended.	8.4 Qualsiasi sessione amministrativa diretta o remota su un firewall non deve visualizzare l'ultimo utente a effettuare l'accesso e deve essere disconnessa quando incustodita.
8.5 Internal hardware firewalls (where used) that protect Johnson & Johnson Information shall be configured and managed in accordance with these Johnson & Johnson Supplier Information Security Requirements.	8.5 I firewall hardware interni (ove utilizzati) che proteggono le Informazioni di Johnson & Johnson devono essere configurati e gestiti in conformità con i presenti Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson.

8.6 Supplier laptops, desktops and workstations shall have a software firewall installed and configured to block all inbound traffic other than that required for business purposes, and shall not be capable of being disabled, modified or updated by unauthorized personnel.	8.6 I portatili, i desktop e le workstation dei fornitori devono avere un firewall software installato e configurato per bloccare tutto il traffico in entrata oltre a quello richiesto per scopi aziendali e non devono essere in grado di essere disabilitati, modificati o aggiornati da personale non autorizzate.
8.7 All connections between an external network (including, but not limited to the Internet) and Supplier's internal network must employ a firewall and intrusion detection (or prevention) capabilities. The IDS/IPS capabilities may be included in the firewall devices and/or separate systems.	8.7 Tutte le connessioni tra una rete esterna (incluso Internet, a titolo esemplificativo ma non esaustivo) e la rete interna del Fornitore devono impiegare un firewall e una capacità di rilevamento (o prevenzione) delle intrusioni. Le funzionalità IDS/IPS possono essere incluse nei dispositivi firewall e/o nei sistemi separati.
8.8 IDS/IPS systems shall not be disabled, shall update signatures used to identify malicious behavior regularly, shall provide alerts when significant events are identified and shall block anomalous traffic where possible.	8.8 I sistemi IDS/IPS non devono essere disabilitati, devono aggiornare le firme utilizzate per identificare regolarmente il comportamento dannoso, devono fornire avvisi quando vengono identificati eventi significativi e devono bloccare il traffico anomalo laddove possibile.
8.9 Before changes are made to the perimeter of Supplier's network (e.g., a new Internet connection, adding a new physical site to the network), Supplier shall perform a risk assessment, ensure the change meets applicable policies (including, but not limited to these Johnson & Johnson Supplier Information Security Requirements) and be approved by Supplier's Information Security Officer or authorized delegate.	8.9 Prima che vengano apportate modifiche al perimetro della rete del Fornitore (per es. una nuova connessione Internet, l'aggiunta di un nuovo sito fisico alla rete), il Fornitore eseguirà una valutazione dei rischi, garantirà che la modifica soddisfi le politiche applicabili (inclusi, a titolo esemplificativo ma non esaustivo, i presenti Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson) e sarà approvata dal Responsabile della sicurezza delle informazioni del Fornitore o da un delegato autorizzato.
9 ACCESS CONTROL	**9 CONTROLLO DEGLI ACCESSI**
BUSINESS REQUIREMENTS FOR ACCESS CONTROL	**REQUISITI AZIENDALI PER IL CONTROLLO DEGLI ACCESSI**
9.1 Supplier shall have an access control policy and limit authorized employees, contractors and other individual's access to Supplier facilities, secure areas, and Computing and Network Resources to only those individuals	9.1 Il Fornitore dovrà disporre di una politica di controllo degli accessi e limitare l'accesso di dipendenti autorizzati, appaltatori e altri soggetti alle strutture del Fornitore, alle aree sicure e alle Risorse informatiche e di rete solo a coloro che hanno un accordo valido in vigore di

who have a valid non-disclosure agreement in effect and a business need for access.	non divulgazione e che necessitano dell'accesso aziendale.
9.2 Supplier management shall approve everyone's access to Supplier facilities, secure areas (e.g., data centers, telecommunication closets, etc.) and Computing and Network Resources to protect against unauthorized access.	9.2 La gestione dei fornitori deve approvare l'accesso di tutti alle strutture dei Fornitori, alle aree sicure (per es. centri dati, armadi per le telecomunicazioni, ecc.) e alle Risorse informatiche e di rete per proteggerle dall'accesso non autorizzato.
9.3 Access controls shall require positive identification and authentication of individuals. Biometric authentication processes shall not be used as the sole means for authenticating an individual to Computing and Network Resources.	9.3 I controlli di accesso devono richiedere l'identificazione e l'autenticazione positiva dei soggetti. I processi di autenticazione biometrica non devono essere utilizzati come unico mezzo per autenticare un soggetto presso le Risorse informatiche e di rete.
USER ACCESS MANAGEMENT	**GESTIONE DELL'ACCESSO UTENTE**
9.4 Privileges granted to an individual shall be the minimal set required for the performance of his or her job in a timely and efficient manner and only for the duration of the need.	9.4 I privilegi concessi a un soggetto saranno i minimi necessari per lo svolgimento del suo lavoro in modo tempestivo ed efficiente e solo per la durata dell'esigenza.
9.5 Management shall approve or deny all requests for elevated privileges.	9.5 La dirigenza deve approvare o negare tutte le richieste di privilegi elevati.
9.6 Individuals shall be required to authenticate prior to the exercise of any elevated privileges (although the same identity and means of authentication may be used).	9.6 Gli individui devono autenticarsi prima dell'esercizio di qualsiasi privilegio elevato (sebbene possano essere utilizzati la stessa identità e gli stessi mezzi di autenticazione).
9.7 Elevated privileges shall be actively managed such that privileges shall be reviewed periodically and revoked when no longer needed.	9.7 I privilegi elevati devono essere gestiti attivamente in modo tale che i privilegi vengano riesaminati periodicamente e revocati quando non sono più necessari.
9.8 Passwords and PINs and other information used for authentication (e.g., shared secrets) shall be encrypted in accordance with these Johnson & Johnson Supplier Information Security Requirements.	9.8 Le password e i PIN e altre informazioni utilizzate per l'autenticazione (per es. segreti condivisi) devono essere crittografati in conformità con i presenti Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson.
9.9 Passwords and PINs shall be delivered in a confidential manner that requires the recipient to prove their identity before the password/PIN is received.	9.9 Le password e i PIN devono essere consegnati in modo riservato e il destinatario deve dimostrare la propria identità prima di ricevere la password/il PIN.
9.10 Passwords and PINs shall never be delivered in conjunction with their associated	9.10 Le password e i PIN non saranno mai consegnati insieme al loro ID utente associato

User ID via the same medium at the same time unless confidentiality of the delivery and proof of recipient identity is provided using industry standard public key cryptography as defined in section 10.	tramite lo stesso mezzo e allo stesso tempo, a meno che la riservatezza della consegna e la prova dell'identità del destinatario non siano fornite utilizzando un sistema di crittografia a chiave pubblica del settore, così come definito nella sezione 10.
9.11 Temporary, reset or initial passwords/PINs shall be unique for everyone, shall be required to change upon first use and shall not be reused for at least three (3) months.	9.11 Password/PIN temporanei, reimpostati o iniziali saranno unici per tutti, dovranno essere modificati al primo utilizzo e non dovranno essere riutilizzati per almeno tre (3) mesi.
9.12 Proper proof of identification shall be provided and verified before a password or PIN is changed.	9.12 Deve essere fornita e verificata una corretta prova di identificazione prima di modificare una password o un PIN.
9.13 Default passwords/PINs shall be changed during or immediately upon the completion of the installation process.	9.13 Le password/i PIN predefiniti devono essere modificati durante o immediatamente dopo il completamento del processo di installazione.
9.14 Compromised accounts and accounts suspected of having been compromised shall be disabled within twenty-four (24) hours.	9.14 I conti compromessi e quelli che si sospetta siano stati compromessi devono essere disattivati entro ventiquattro (24) ore.
9.15 Upon an individual's resignation or termination, the individual's accounts shall be disabled and all shared passwords and PINs under that individual's control (e.g., service account password) shall be changed no later than 72 hours after termination.	9.15 In caso di dimissioni o revoca di un soggetto, i suoi account saranno disabilitati e tutte le password e i PIN condivisi sotto il suo controllo (per es. password dell'account di servizio) saranno modificati entro e non oltre 72 ore dalla cessazione.
9.16 Supplier shall review and re-approve access privileges semi-annually for Systems containing Johnson & Johnson Information and In-Scope Applications, and annually for all other Systems. Events such as changes in title or role shall trigger additional review and re-approval.	9.16 Il Fornitore dovrà rivedere e riapprovare i privilegi di accesso semestrale per i Sistemi contenenti Informazioni e Applicazioni nell'ambito di Johnson & Johnson e annualmente per tutti gli altri Sistemi. Eventi come modifiche del titolo o del ruolo devono dare avvio a una revisione e a una nuova approvazione supplementari.
NETWORK ACCESS CONTROL	**CONTROLLO DEGLI ACCESSI ALLA RETE**
9.17 Supplier shall limit access to Supplier's network to only those employees, contractors and other users who have a business need for access.	9.17 Il Fornitore limiterà l'accesso alla rete del Fornitore solo a quei dipendenti, appaltatori e altri utenti che hanno un'esigenza aziendale di avere accesso.
9.18 All remote access or wireless access communication sessions shall make use of	9.18 Tutte le sessioni di comunicazione con accesso remoto o wireless devono utilizzare

network protocols that protect the confidentiality and integrity of all data in transport. These protocols shall adhere to all applicable cryptographic standards for algorithms and key lengths specified in these Johnson & Johnson Supplier Information Security Requirements.	protocolli di rete che proteggano la riservatezza e l'integrità di tutti i dati trasferiti. Questi protocolli devono rispettare tutti gli standard crittografici applicabili per gli algoritmi e le lunghezze delle chiavi specificati nei presenti Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson.
9.19 All remote access and wireless network services that grant unrestricted access to Supplier networks shall ensure the individual seeking services is identified and strongly authenticated before access is granted.	9.19 Tutti i servizi di accesso remoto e di rete wireless che concedono l'accesso illimitato alle reti del Fornitore devono garantire che il soggetto che cerca i servizi sia identificato e debitamente autenticato prima di concedere l'accesso.
• Remote access to Supplier's network that provides access to either Johnson & Johnson Information or Server Systems or In-Scope Applications containing Johnson & Johnson Information, shall employ Two-factor authentication using: a) a physical or protected token that contains cryptographic materials in combination with a passphrase or other factor that only the user knows; or b) a compliant password in combination with a one-time security code from a Supplier-approved service.	• L'accesso remoto alla rete del Fornitore che fornisce l'accesso alle Informazioni di Johnson & Johnson o ai Sistemi server o alle Applicazioni nell'ambito contenenti le Informazioni di Johnson & Johnson, utilizzerà l'autenticazione a due fattori ricorrendo: a) un token fisico o protetto che contiene materiali crittografici in combinazione con una frase d'accesso o un altro fattore che solo l'utente conosce, oppure b) una password conforme in combinazione con un codice di sicurezza OTP rilasciato da un servizio approvato dal Fornitore.
• In-facility wireless access to Supplier's network or remote access to Supplier's network that provides access to Johnson & Johnson Information, or access to Server Systems or In-Scope Applications containing Johnson & Johnson Information, shall employ Two-factor authentication using: a) a physical or protected software token that contain cryptographic materials in combination with a passphrase or other factor that only the user knows; or b) a compliant password in combination with a one-time security code from a Supplier approved service.	• L'accesso wireless interno alla rete del Fornitore o l'accesso remoto alla rete del Fornitore che fornisce l'accesso alle Informazioni di Johnson & Johnson o accesso ai Sistemi server o alle Applicazioni nell'ambito contenenti le Informazioni di Johnson & Johnson, utilizzerà l'autenticazione a due fattori ricorrendo: a) un token fisico o protetto che contiene materiali crittografici in combinazione con una frase d'accesso o un altro fattore che solo l'utente conosce, oppure b) una password conforme in combinazione con un codice di sicurezza OTP rilasciato da un servizio approvato dal Fornitore.
9.20 Direct diagnostic access to Supplier Systems or networks, for the purpose of monitoring or problem diagnosis and/or repair, shall not allow:	9.20 L'accesso diagnostico diretto ai sistemi o alle reti dei fornitori, a fini del monitoraggio o della diagnosi e/o della riparazione dei problemi, non consentirà:
• Elevated or administrator privilege without explicit enablement and supervision by authorized personnel	• Privilegio elevato o amministratore senza autorizzazione e supervisione esplicite da parte del personale autorizzato

• Access to any other location or service on Supplier's network	• Accesso a qualsiasi altra sede o servizio sulla rete del Fornitore
• Access to Johnson & Johnson Information or networks	• Accesso alle informazioni o alle reti di Johnson & Johnson
9.21 No User System shall be connected to more than one network at the same time in such a way that it will route or bridge traffic from one network to another.	9.21 Nessun sistema utente deve essere collegato a più di una rete contemporaneamente in modo da instradare o collegare il traffico da una rete all'altra.
9.22 Audio or audiovisual teleconferencing equipment shall be configured to not answer any incoming connections without human action to establish a connection.	9.22 L'apparecchiatura di teleconferenza audiovisiva deve essere configurata in modo da non rispondere ad alcuna connessione in entrata senza la presenza di una azione umana per stabilire una connessione.
OPERATING SYSTEM and IN-SCOPE APPLICATION ACCESS CONTROL	**SISTEMA OPERATIVO e CONTROLLO DEGLI ACCESSI CON APPLICAZIONE NELL'AMBITO**
Supplier shall implement the following access control mechanisms for all User Systems, Server Systems and Network Device operating systems, and In-Scope Applications:	*Il Fornitore dovrà implementare i seguenti meccanismi di controllo dell'accesso per tutti i Sistemi utente, i Sistemi server e i Sistemi operativi dei Dispositivi di rete e le Applicazioni nell'ambito:*
9.23 Access controls shall require positive identification and authentication of individuals. Biometric authentication processes shall not be used as the sole means for authenticating an individual, excluding the ability to unlock a Mobile Computing Device where the biometric mechanism has been evaluated and approved by the Supplier Information Security Officer.	9.23 I controlli di accesso devono richiedere l'identificazione e l'autenticazione positiva dei soggetti. I processi di autenticazione biometrica non devono essere utilizzati come unico mezzo per l'autenticazione di un soggetto, esclusa la capacità di sbloccare un Dispositivo informatico mobile in cui il meccanismo biometrico sia stato valutato e approvato dal Responsabile della sicurezza delle informazioni del fornitore.
9.24 Authorization decisions shall be based on an individual's authenticated identity and the privileges granted to that individual.	9.24 Le decisioni di autorizzazione si baseranno sull'identità autenticata di un soggetto e sui privilegi concessigli.
9.25 User access privileges shall be disabled when not used for 180 days unless an access control list review is conducted every 180 days and accounts no longer requiring access are disabled.	9.25 I privilegi di accesso utente devono essere disabilitati se non utilizzati per 180 giorni, a meno che non venga eseguita una revisione della lista di controllo degli accessi ogni 180 giorni e che siano disabilitati gli account che non richiedono più l'accesso.
9.26 Individual user passwords shall be of high quality and follow length, complexity, aging, re-use, and other restrictions as defined by NIST	9.26 Le password dei singoli utenti devono essere di alta qualità e rispettare la lunghezza, la complessità, l'invecchiamento, il riutilizzo e

SP800-63B, ISO27002, or other globally recognized standards bodies agreed to by Johnson & Johnson. Mobile Computing Devices that contain, or are used to access, Johnson & Johnson Information shall require a password or biometric mechanism to obtain access.	altre restrizioni definite da NIST SP800-63B, ISO27002 o altri organismi di normazione riconosciuti a livello globale concordati da Johnson & Johnson. I dispositivi informatici mobili che contengono o sono utilizzati per accedere alle Informazioni di Johnson & Johnson richiedono una password o un meccanismo biometrico per ottenere l'accesso.
9.27 Individual passwords and PINs must expire and be changed regularly, but no less frequently than every 180 days. Service account passwords may have a longer expiration period as determined by Supplier. Passwords and PINs may not be reused for a reasonable amount of time or number of password iterations.	9.27 Le password e i PIN individuali devono scadere ed essere modificati regolarmente, ma con una frequenza non inferiore a 180 giorni. Le password dell'account di servizio potrebbero avere un periodo di scadenza più lungo, come determinato dal fornitore. Le password e i PIN non possono essere riutilizzati per un ragionevole periodo di tempo o un numero di iterazioni delle password.
9.28 Multiple consecutive failed attempts to authenticate using a password within a sufficient maximum period shall result in the account being locked or temporarily disabled for an amount of time sufficient to render automated guessing difficult and unlikely to succeed.	9.28 Più tentativi consecutivi di autenticazione non riusciti utilizzando una password entro un periodo massimo sufficiente determineranno il blocco o la disattivazione temporanea dell'account per un periodo di tempo sufficiente a rendere difficile e improbabile il successo dell'automatizzazione.
9.29 Where technically possible, default account names shall be changed.	9.29 Ove tecnicamente possibile, i nomi predefiniti degli account devono essere modificati.
9.30 Excluding Mobile Computing Devices, password authentication shall ensure that passwords and PINs are not displayed to individuals in readable form at any time. Mobile Computing Devices may display individual characters in a readable form which must become unreadable at entry of the next character.	9.30 Escludendo i dispositivi informatici mobili, l'autenticazione tramite password garantirà che password e PIN non vengano mostrati ai soggetti in qualsiasi momento in forma leggibile. I dispositivi mobili possono visualizzare singoli caratteri in una forma leggibile che deve diventare illeggibile al momento dell'inserimento del carattere successivo.
9.31 Passwords and PINs shall be changed whenever there is any indication of password compromise.	9.31 Le password e i PIN devono essere cambiati ogni volta che vi sia qualsiasi indicazione di compromissione della password.
9.32 Passwords and PINs shall never be cached.	9.32 Le password e i PIN non devono mai essere memorizzati nella cache.
9.33 The user interface shall lock after a sufficient maximum period of inactivity and	9.33 L'interfaccia utente si bloccherà dopo un periodo massimo sufficiente di inattività e

shall require the user to re-authenticate to unlock the interface.	richiederà all'utente di eseguire nuovamente l'autenticazione per sbloccare l'interfaccia.
10 CRYPTOGRAPHY	**10 CRIPTOGRAFIA**
10.1 Where encryption is required by Johnson & Johnson for the protection of Johnson & Johnson Information, Supplier shall implement encryption using non-proprietary encryption algorithms in accordance with those standards set forth in the current versions of the FIPS 140 series or the NIST Special Publication 800 series.	10.1 Laddove la crittografia sia richiesta da Johnson & Johnson per la protezione delle Informazioni di Johnson & Johnson, il Fornitore dovrà implementare la crittografia utilizzando algoritmi di criptografia non proprietari in conformità con le norme stabilite nelle versioni attuali della serie FIPS 140 o della serie NIST Special Publication 800.
10.2 Supplier shall have a process and controls in place to ensure symmetric encryption keys and asymmetric private keys are encrypted in transmission and storage, are protected from unauthorized access, and are secured.	10.2 Il Fornitore deve disporre di un processo e di controlli per garantire che le chiavi di crittografia simmetrica e le chiavi private asimmetriche crittografate in trasmissione e archiviazione, siano protette da accessi non autorizzati e messe in sicurezza.
10.3 Segregation of duties shall be instituted such that administrative personnel with read access to the keys are distinct from those individuals with read access to the ciphertext.	10.3 La separazione dei compiti deve essere istituita in modo tale che il personale amministrativo con accesso in lettura alle chiavi sia distinto dalle persone con accesso in lettura al testo cifrato.
10.4 Systems employing symmetric encryption keys shall have the capability to change/update the key(s).	10.4 I sistemi che impiegano chiavi di crittografia simmetrica avranno la possibilità di modificare/aggiornare la/le chiave/i.
10.5 Default vendor-generated symmetric encryption keys shall always be changed to non-default values, such that the changed values are not known to the vendor's other customers and not known to the vendor unless required by intended function.	10.5 Le chiavi di crittografia simmetrica generate dal fornitore predefinito devono sempre essere modificate in valori non predefiniti, in modo che i valori modificati non siano noti agli altri clienti del fornitore e non siano noti al fornitore, a meno che non sia richiesto dalla funzione prevista.
10.6 Symmetric encryption keys used to encrypt backups shall be stored separately from the data being backed up.	10.6 Le chiavi di crittografia simmetrica utilizzate per crittografare i backup devono essere archiviate separatamente dai dati dei quali si esegue il backup.
10.7 Supplier shall use PKI resources from reputable, trusted providers to protect Johnson & Johnson Information and other	10.7 Il Fornitore utilizzerà le risorse PKI di fornitori rispettabili e affidabili per proteggere le Informazioni di Johnson & Johnson e altre

sensitive information (such as protecting passwords during transmission with TLS).	informazioni sensibili (come la protezione delle password durante la trasmissione con TLS).
11 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE	**11 ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI INFORMATIVI**
SECURITY OF SYSTEM FILES	**SICUREZZA DEI FILE DI SISTEMA**
Supplier shall implement the following system security controls on all Computing and Network Resources:	*Il Fornitore dovrà implementare i seguenti controlli di sicurezza del sistema su tutte le Risorse informatiche e di rete:*
11.1 All software installations on User Systems, Server Systems and Network Devices shall be evaluated for risk and be approved by the Supplier's Information Security Officer or delegate.	11.1 Tutte le installazioni di software su Sistemi utente, Sistemi server e Dispositivi di rete devono essere valutate in relazione al rischio e approvate dal Responsabile della sicurezza delle informazioni del Fornitore o dal suo delegato.
11.2 Software updates and patches shall be researched, tested and verified by appropriate Supplier personnel before installation.	11.2 Gli aggiornamenti e le patch del software devono essere studiati, testati e verificati dal personale appropriato del Fornitore prima dell'installazione.
SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	**SICUREZZA NELLO SVILUPPO E NEI PROCESSI DI SUPPORTO**
11.3 Supplier shall have a System Development Lifecycle (SDLC) for the development and deployment of Systems and In-Scope Applications, which incorporates activities and deliverables to ensure security requirements are met.	11.3 Il Fornitore dovrà disporre di un Ciclo di sviluppo del sistema (SDLC) per la messa a punto e la distribuzione di Sistemi e Applicazioni nell'ambito che preveda attività e risultati al fine di garantire che vengano soddisfatti i requisiti di sicurezza.
11.4 Secure coding practices such as those dictated by the OWASP Secure Coding Practices reference shall be utilized for internet-facing websites/web applications hosting Johnson & Johnson Information, including but not limited to input/output validation, error and exception handling, cryptography, cookie and session management, and system configuration (e.g., default credentials/files shall be removed or disabled).	11.4 Le pratiche di codifica sicura, come quelle dettate dal riferimento delle pratiche di codifica sicura OWASP, devono essere utilizzate per i siti web/le applicazioni web che ospitano le Informazioni di Johnson & Johnson, tra cui, a titolo esemplificativo ma non esaustivo, la convalida dell'input/output, la gestione degli errori e delle eccezioni, la crittografia, la gestione dei cookie e delle sessioni e la configurazione del sistema (per es. le

	credenziali/file predefiniti devono essere rimossi o disabilitati).
11.5 Supplier shall perform testing to ensure security requirements are met, including the testing of interfaces among systems and system components.	11.5 Il Fornitore deve eseguire test per garantire che vengano soddisfatti i requisiti di sicurezza, compresi i test delle interfacce tra sistemi e componenti di sistema.
11.6 Supplier shall ensure Johnson & Johnson production data is not used in non-production environments (e.g., development or test) unless the data is protected in compliance with these Johnson & Johnson Supplier Information Security Requirements.	11.6 Il Fornitore dovrà garantire che i dati di produzione di Johnson & Johnson non vengano utilizzati in ambienti non di produzione (per es. sviluppo o test), a meno che i dati non siano protetti in conformità con i presenti Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson.
12 INFORMATION SECURITY INCIDENT MANAGEMENT	**12 GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI**
12.1 Supplier shall have a formal security incident monitoring, reporting and response capability to identify, report and appropriately respond to known or suspected security incidents, including any unauthorized access, acquisition, use, disclosure or destruction of Johnson & Johnson Information. This capability shall ensure notification is provided to Johnson & Johnson of any known or suspected compromise of Johnson & Johnson Information or In-Scope Applications within 24 hours.	12.1 Il Fornitore dovrà disporre di una capacità formale di monitoraggio, segnalazione e risposta degli incidenti di sicurezza, al fine di identificare, segnalare e rispondere adeguatamente agli incidenti di sicurezza noti o sospetti, compreso qualsiasi accesso, acquisizione, uso, divulgazione o distruzione non autorizzati delle Informazioni di Johnson & Johnson. Questa possibilità deve garantire che venga fornita notifica a Johnson & Johnson circa qualsiasi compromissione nota o sospetta delle Informazioni o delle Applicazioni nell'ambito di Johnson & Johnson entro 24 ore.
12.2 Supplier shall ensure an assessment report is created when a User System is lost or stolen, which identifies the compromise or potential compromise of information. If Johnson & Johnson Information is included in the assessment report, the Supplier must notify Johnson & Johnson or the applicable Johnson & Johnson Affiliate within 24 hours.	12.2 Il Fornitore dovrà garantire che venga creata una relazione di valutazione quando venga perso o sottratto un Sistema utente che identifichi la compromissione o la potenziale compromissione delle informazioni. Se le Informazioni di Johnson & Johnson sono incluse nella relazione di valutazione, il Fornitore deve informare Johnson & Johnson o l'appropriata affiliata di Johnson & Johnson entro 24 ore.

13 BUSINESS CONTINUITY MANAGEMENT	**13 GESTIONE DELLA CONTINUITÀ AZIENDALE**
13.1 Supplier shall identify requirements for, and institute and practice, an Information Systems Continuity of Business and Disaster Recovery Plan that will prevent catastrophic data loss and ensure timely restoration of network and computing services in the event of system failure, damage or destruction.	13.1 Il Fornitore deve identificare i requisiti, e istituire e praticare, un Piano di continuità dei sistemi informatici di business e di disaster recovery che prevenga la perdita di dati catastrofici e garantisca il ripristino tempestivo dei servizi di rete e informatici in caso di guasto, danno o distruzione del sistema.
13.2 Supplier shall ensure the plan is tested no less frequently than once every two years to ensure it can be executed correctly and efficiently.	13.2 Il Fornitore deve garantire che il piano sia testato con frequenza non inferiore a una volta ogni due anni per garantire che possa essere eseguito in modo corretto ed efficiente.
14 COMPLIANCE	**14 CONFORMITÀ**
14.1 Supplier shall comply with any legal or regulatory requirements where applicable in the performance of services for Johnson & Johnson or any Johnson & Johnson Affiliate.	14.1 Il Fornitore dovrà rispettare qualsiasi requisito legale o normativo, laddove applicabile, nell'erogazione di servizi per Johnson & Johnson o qualsiasi Affiliata di Johnson & Johnson.
14.2 Supplier shall ensure compliance with relevant legislation, regulations and contractual clauses, to ensure the protection of Johnson & Johnson Information.	14.2 Il Fornitore dovrà garantire la conformità con la legislazione, le normative e le clausole contrattuali pertinenti, al fine di garantire la protezione delle Informazioni di Johnson & Johnson.
14.3 Supplier shall allow and support the completion of periodic assessments by Johnson & Johnson or a Johnson & Johnson Affiliate to determine compliance with these Johnson & Johnson Supplier Information Security Requirements.	14.3 Il Fornitore dovrà consentire e supportare il completamento di valutazioni periodiche da parte di Johnson & Johnson o di una sua Affiliata, al fine di stabilire la conformità con i presenti Requisiti sulla sicurezza delle informazioni dei fornitori di Johnson & Johnson.