Stemma dell'Ospedale di S. Maria della Misericordia di Perugia

Azienda Ospedaliera di Perugia

Direzione Generale e Sede Amministrativa: Piazzale Giorgio Menghini, 8/9 – 06129 PERUGIA
Sede Legale: Ospedale Santa Maria della Misericordia – Sant'Andrea delle Fratte – 06132 PERUGIA

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO

7 NOV. 2019 N° 1011

OGGETTO: Approvazione del Disciplinare per la richiesta di accessi da remoto a dati e risorse aziendali (VPN).

IL COMMISSARIO STRAORDINARIO

VISTA la proposta di deliberazione del 04/11/2019 N° 5 di pari oggetto predisposta della competente Articolazione Organizzativa e allegata a questo atto come parte integrante:

ACQUISITI I PARERI FAVOREVOLI
DEL DIRETTORE AMMINISTRATIVO E DEL DIRETTORE SANITARIO.

D E L I B E R A

DI FARE INTEGRALMENTE PROPRIA LA MENZIONATA PROPOSTA DI DELIBERA E DI DISPORRE QUINDI COSI' COME IN ESSA INDICATO.

IL COMMISSARIO STRAORDINARIO (Dr. Antonio Onnis)

IL DIRETTORE AMMINISTRATIVO (Dott. Matteo Sammartino)

IL DIRETTORE SANITARIO (Dr. Luca Bianciardi)

Stemma dell'Ospedale di S. Maria della Misericordia di Perugia

Azienda Ospedaliera di Perugia

Direzione Generale e Sede Amministrativa: Piazzale Giorgio Menghini, 8/9 – 06129 PERUGIA
Sede Legale: Ospedale Santa Maria della Misericordia – Sant'Andrea delle Fratte – 06132 PERUGIA

SISTEMI INFORMATICI E TRANSIZIONE ALL'AMMINISTRAZIONE DIGITALE

PROPOSTA DI DELIBERA DEL 04/11/2019 N° 5

OGGETTO: Approvazione del Disciplinare per la richiesta di accessi da remoto a dati e risorse aziendali (VPN).

PREMESSO:

che con l'entrata in vigore del Regolamento Generale sulla Protezione dei Dati (GDPR) (UE 679/2016 - General Data Protection Regulation), l'Azienda Ospedaliera di Perugia ha avviato un percorso di aggiornamento e rafforzamento delle proprie politiche di sicurezza informatica al fine di garantire la riservatezza e l'integrità dei dati trattati;

che al fine di innalzare i livelli di sicurezza, uno degli interventi prioritari è regolamentare e monitorare i collegamenti da e verso le reti esterne;

che, a questo scopo, la S.S. Sistemi Informatici e Transizione all'Amministrazione Digitale ha configurato un'infrastruttura tecnologica VPN (Virtual Private Network) di ultima generazione, che permette di creare dei canali di comunicazione sicuri e cifrati, verso i soggetti titolati ed autorizzati a collegarsi dall'esterno

che per definire quali soggetti debbano essere autorizzati, i relativi permessi, privilegi e ambiti operativi, la S.S. Sistemi Informatici e Transizione all'Amministrazione Digitale ha redatto un "Disciplinare per la richiesta di accessi da remoto a dati e risorse aziendali (VPN)" e sottoposto il documento al vaglio del DPO (Data Protection Officer) e dell'Ufficio Privacy.

PRESO ATTO:

che in data 28/10/2019 il DPO ha approvato il documento ritenendo il Disciplinare "una misura utile e di buon senso, oltre che migliorativa della protezione dei *dati personali e della tracciabilità.*"

che è opportuno pertanto adottare il Disciplinare e darne massima diffusione ai dirigenti apicali e a tutti i soggetti interessati;

Sulla base delle motivazioni sopra esposte, vista la vigente normativa:

SI PROPONE DI DELIBERARE QUANTO SEGUE:

1) Approvare il "Disciplinare per la richiesta di accessi da remoto a dati e risorse aziendali (VPN)", allegato alla presente quale parte integrante e sostanziale, che entra in vigore nella data di approvazione del presente atto;

2) Dichiarare, dalla stessa data di approvazione, l'inefficacia dei previgenti Regolamenti/Disciplinari in materia;

3) Affidare al Dirigente della S.S. Sistemi Informatici e Transizione all'Amministrazione Digitale i seguenti compiti:

   - Proporre modifiche al Disciplinare in caso di variazioni normative e/o organizzative.
   - Adottare le procedure operative necessarie all'applicazione del presente Disciplinare.
   - Pubblicare sul sito Aziendale il Disciplinare e le relative procedure e darne massima diffusione;

4) Dare atto che la presente delibera non è sottoposta a controllo Regionale;

5) Trasmettere il presente atto al Collegio Sindacale.

Il Dirigente
Sistemi Informatici e Transizione
all'Amministrazione Digitale
Ing. Alfiero Ortali

ALLEGATO

Azienda Ospedaliera di Perugia

Sistemi Informatici e Transizione all'Amministrazione Digitale

Ottobre 2019

Sommario

1. SCOPO 2
2. DESTINATARI 2
3. RIFERIMENTI 2
3.1 ALLEGATI 2
3.2 NORMATIVE E STANDARD DI RIFERIMENTO 3
4. ACRONIMI E DEFINIZIONI 3
5. REVISIONI 3
6. CONDIZIONI DI ACCESSO 3
7. MODALITÀ DI ATTIVAZIONE VPN 4
7.1 DIPENDENTE AREA AMMINISTRATIVA 4
7.2 DIPENDENTE AREA SANITARIA 5
7.3 SOGGETTO ESTERNO CON CONTRATTO GESTITO DAL SITAD 5
7.4 SOGGETTO ESTERNO CON CONTRATTO GESTITO DALLA BIOINGEGNERIA 7
7.5 SOGGETTO ESTERNO DIVERSO DAI CASI SOPRA CITATI 8
8. MODIFICA VPN 9
9. DISATTIVAZIONE VPN 9
10. MONITORAGGIO VPN 9
ALLEGATO 1 10
ALLEGATO 2 12
ALLEGATO 3 14
ALLEGATO 4 16

Disciplinare per la richiesta di accessi da remoto a dati e risorse aziendali (VPN)

1. Scopo

Il presente documento ha l'obiettivo di definire le modalità operative per la gestione delle richieste di abilitazione delle utenze VPN per l'accesso da remoto all'infrastruttura di rete dell'Azienda Ospedaliera di Perugia, da parte sia di soggetti terzi che di utenti interni.

2. Destinatari

Destinatari del presente documento sono le seguenti Funzioni Aziendali:

- Direzione Generale
- Direzione Medica Ospedaliera
- Direzione Bioingegneria
- Direttori di Dipartimento
- Responsabili di Struttura Complessa
- Sistemi Informativi e Transizione all'Amminsitrazione Digitale
- Ufficio Privacy

3. Riferimenti

I seguenti riferimenti, nella edizione in vigore alla data della presente, fanno parte della stessa nei limiti degli argomenti trattati.

3.1 Allegati

Di seguito la documentazione di riferimento a supporto del presente documento:

- Allegato 1: Modulo di richiesta di accesso remoto per dipendenti
- Allegato 2: Modulo di richiesta di accesso remoto per fornitori esterni di software
- Allegato 3: Modulo di richiesta di accesso remoto per fornitori esterni di dispositivi elettromedicali e software correlati
- Allegato 4: Modulo richiesta accesso remoto per soggetti esterni senza rapporti contrattuali con l'Azienda

3.2 Normative e standard di riferimento

- **ISO/IEC 27001:2013:** Standard Internazionale per la sicurezza digitale
- **AgID:** Misure minime di sicurezza ICT per le Pubbliche Amministrazioni
- **Regolamento UE 679/2016 (GDPR):** General Data Protection Regulation
- **Delibera 493 del 7/3/2018:** Disciplinare per il corretto utilizzo degli strumenti informatici e telematici, Internet e posta elettronica

4. Acronimi e definizioni

Di seguito viene precisato il significato delle definizioni ed abbreviazioni impiegate nel presente documento:

VPN	Virtual Private Network
AO	Azienda Ospedaliera
SC	Struttura Complessa
SITAD	Sistemi Informatici e Transizione all'Amministrazione Digitale
DPO	Responsabile Protezione Dati (anche RPD)

5. Revisioni

Revisione	Data	Descrizione
1	19/10/2019	Prima emissione

6. Condizioni di accesso

L'accesso in VPN ai dati e alle risorse dell'Azienda Ospedaliera è riservato agli utenti autorizzati secondo le modalità di seguito elencate.

Il SITAD si occupa della sicurezza dei collegamenti e del monitoraggio e controllo, in aderenza alla normativa vigente in materia di sicurezza e protezione dati.

Gli accessi VPN sono concessi nominalmente al soggetto richiedente o all'Azienda che necessiti tale collegamento, in modo da rendere tracciabile qualsiasi attività effettuata durante la connessione. L'unica deroga è concessa alle ditte che si avvalgono di sistemi di tracciatura interna, qualora la procedura utilizzata sia esplicitata e concordata con il SITAD.

In ogni caso, il firmatario del modulo di richiesta (Allegato 1) è responsabile della gestione delle credenziali assegnate ed è sua cura custodirle.

Qualora il titolare di una VPN abbia il sospetto che, tramite il suo accesso, siano state eseguite azioni indebile ha l'obbligo di comunicare tempestivamente al SITAD questo sospetto, chiedendo l'immediata disattivazione del collegamento. Il SITAD, in accordo con la Direzione Aziendale e il DPO eseguirà i dovuti controlli.

7. Modalità di attivazione VPN

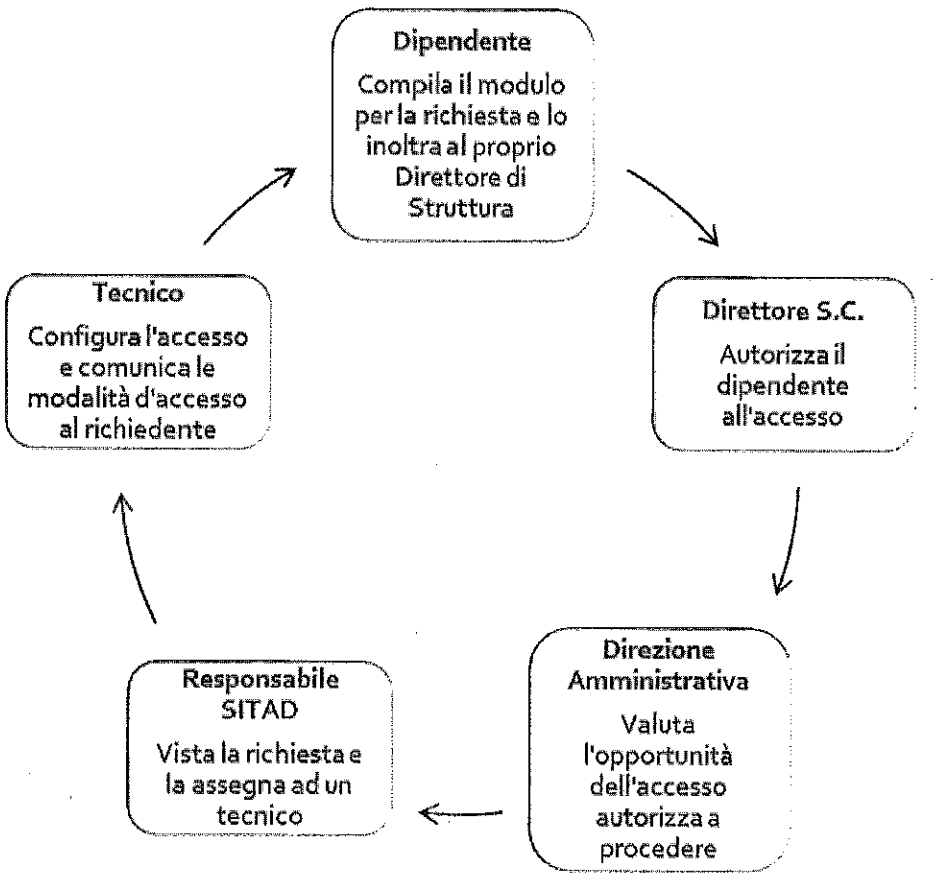
Di seguito lo schema del processo di attivazione VPN.

I processi elencati fanno riferimento ai seguenti casi:

1. Dipendente Area Amministrativa
2. Dipendente Area Sanitaria
3. Soggetto esterno con contratto gestito dal SITAD
4. Soggetto esterno con contratto gestito dalla Bioingegneria
5. Soggetto esterno diverso dai casi sopra citati

7.1 Dipendente Area Amministrativa

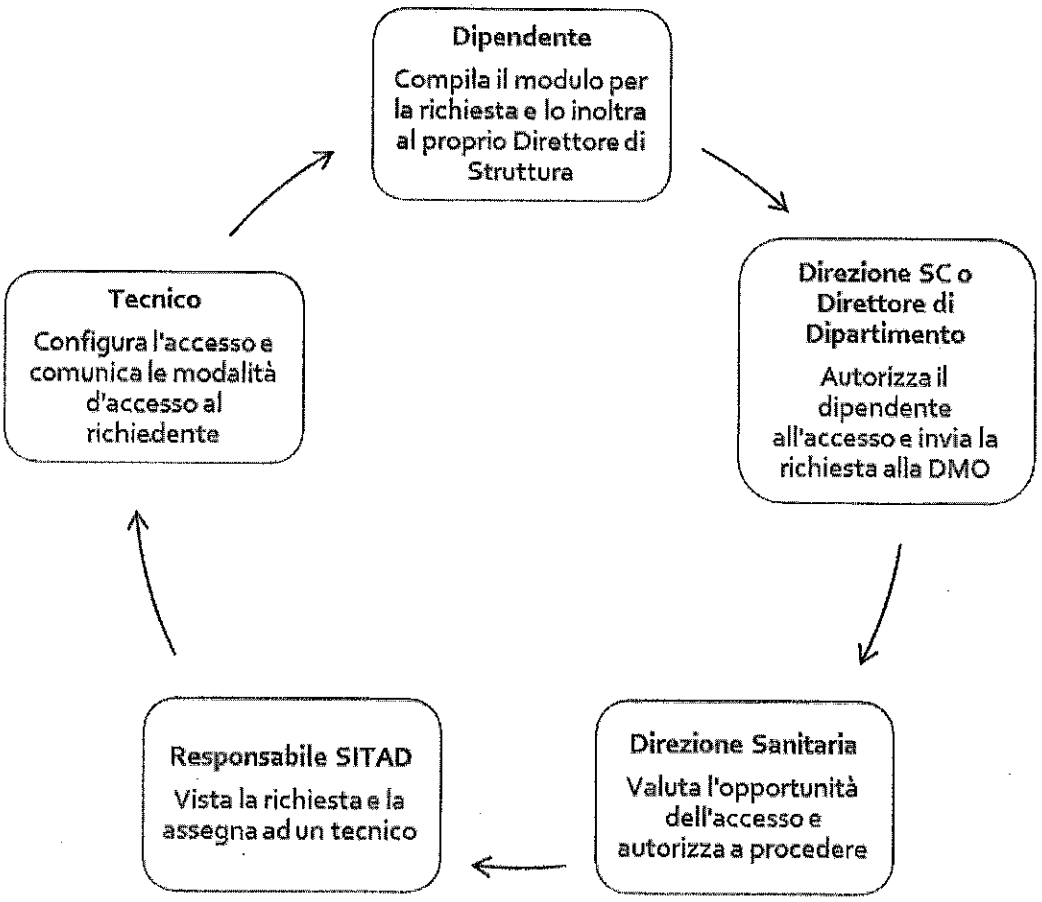
Se un dipendente dell'Area Amministrativa ha necessità di un collegamento VPN per accedere a dati e risorse aziendali dall'esterno (ad esempio per telelavoro o urgenze ben definite), inoltra il modulo (Allegato 1) al proprio responsabile, il quale, qualora autorizzi, indirizza la richiesta da lui sottoscritta alla Direzione Amministrativa. Il Direttore valuta la richiesta e, se ritiene opportuno l'accesso, appone il nulla osta. La segreteria della Direzione inoltra la pratica al SITAD. Il Responsabile SITAD, una volta controllata formalmente la richiesta e vistata, la assegna ad uno dei tecnici per la configurazione. Sarà cura del tecnico stesso contattare il richiedente per comunicare le modalità di accesso e fornire il supporto necessario.



7.2 Dipendente Area Sanitaria

A differenza dell'Area Amministrativa, i dipendenti sanitari hanno necessità e possibilità di accedere a dati sensibili riguardanti la salute dei cittadini e, quindi, sottoposti a maggior tutela dalla normativa vigente.

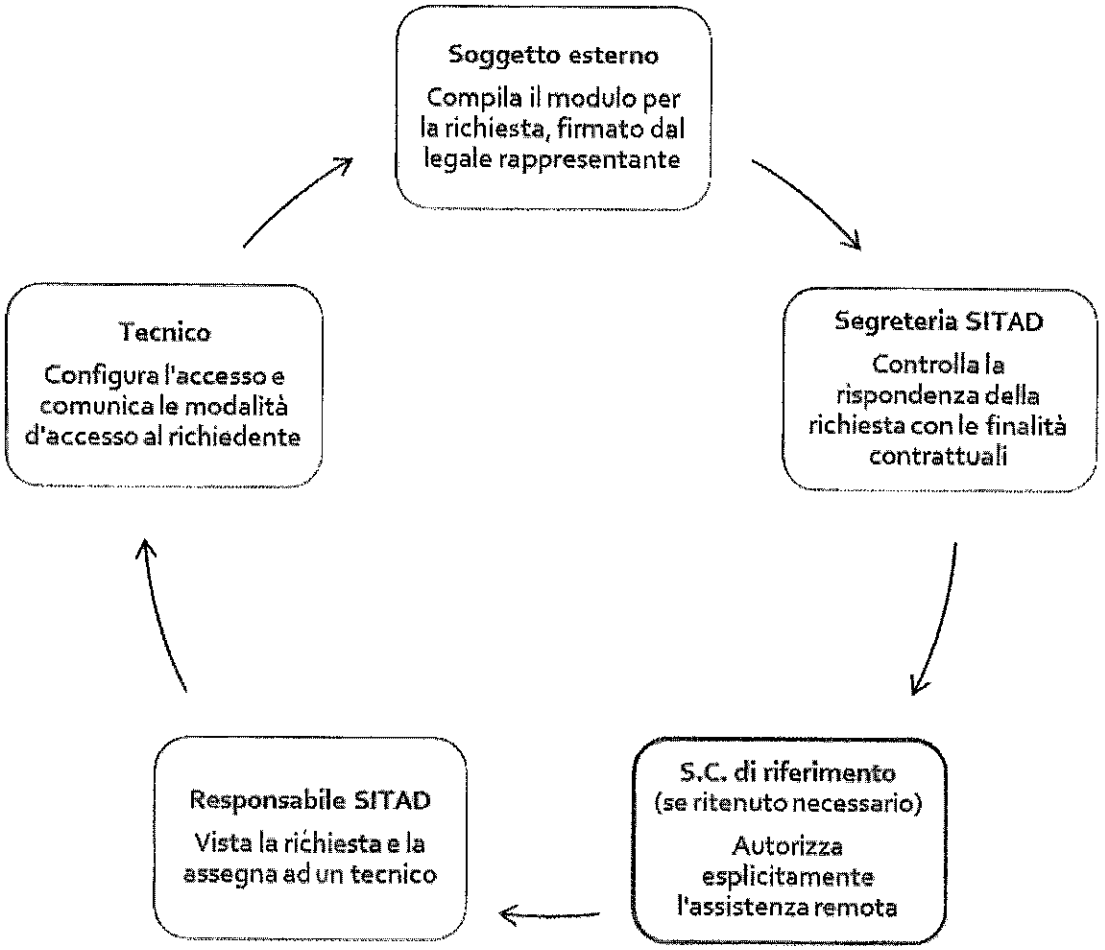
Se un dipendente dell'Area Sanitaria ha necessità di un collegamento VPN, inoltra il modulo (Allegato 1) al proprio Direttore di SC (o Direttore di Dipartimento), il quale, qualora autorizzi, indirizza la richiesta da lui sottoscritta alla Direzione Medica, il cui parere è vincolante per concedere l'autorizzazione. Se la DMO autorizza, inoltra la pratica al Responsabile SITAD, che una volta controllata formalmente la richiesta, appone il proprio visto e la assegna ad uno dei tecnici per la configurazione. Sarà cura del tecnico stesso contattare il richiedente per comunicare le modalità di accesso e fornire il supporto necessario.



7.3 Soggetto esterno con contratto gestito dal SITAD

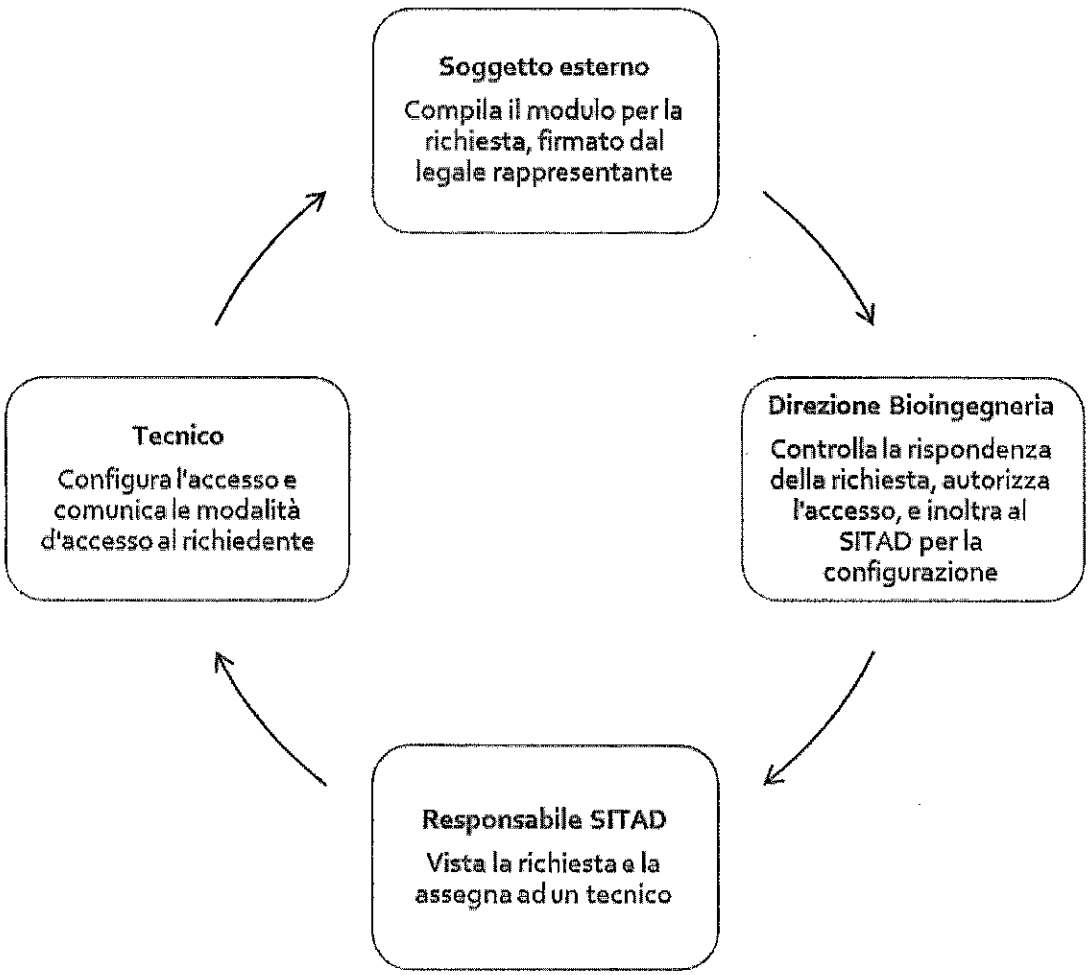
Le ditte esterne che hanno un contratto di assistenza e manutenzione per un software in corso di validità, hanno necessità di attuare controlli ed assistenza da remoto, secondo le specifiche contrattuali. Per formalizzare la richiesta di accesso, al momento della sottoscrizione del contratto o del suo rinnovo, dovrà inviare il modulo (Allegato 2), debitamente compilato e sottoscritto dal legale rappresentante, alla segreteria del SITAD. La segreteria, dopo un primo controllo formale sulla rispondenza tra il contratto e quanto richiesto, invierà la pratica al Responsabile SITAD, il quale apporrà il proprio visto e assegnerà la pratica ad uno dei tecnici per procedere con la configurazione e supporto al fornitore.

Se nel contratto non è presente alcun riferimento all'assistenza remota, il Responsabile SITAD, inoltrerà la pratica al Direttore Esecuzione Contratto o alla S.C. di riferimento per una formale autorizzazione di quanto richiesto, prima di approvare la VPN.



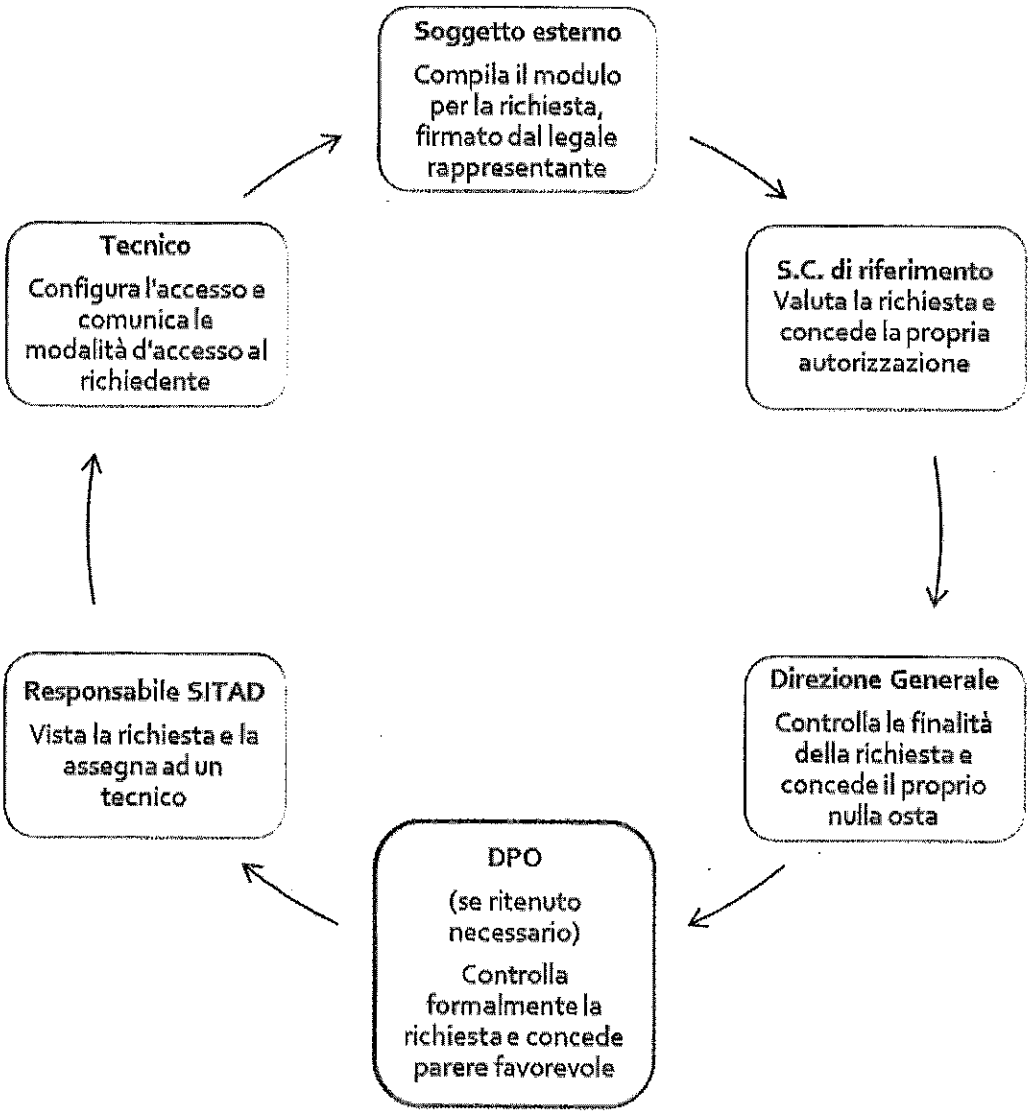
7.4 Soggetto esterno con contratto gestito dalla Bioingegneria

Le ditte esterne che hanno un contratto di assistenza e manutenzione per apparecchiatura elettromedicale (o un software legato ad un'apparecchiatura elettromedicale), hanno necessità di attuare controlli ed assistenza da remoto, secondo le specifiche contrattuali. Per formalizzare la richiesta di accesso, la società dovrà inviare il modulo (Allegato 3), debitamente compilato e sottoscritto dal legale rappresentante, alla Direzione Bioingegneria che, una volta autorizzata la richiesta, la inoltrerà al SITAD. Il Responsabile SITAD apporrà il proprio visto e assegnerà la pratica ad uno dei tecnici per procedere con la configurazione e supporto al fornitore.



7.5 Soggetto esterno diverso dai casi sopra citati

Qualora per esigenze ben documentate e circostanziate, un soggetto esterno (soggetti istituzionali, rappresentante di altri entri, medici di altre Aziende Sanitarie, personale universitario non convenzionato), abbia necessità di accedere a dati e risorse dell'Azienda Ospedaliera, una volta compilato debitamente il modulo (Allegato 4), indirizzerà la richiesta, su carta intestata, alla S.C. di riferimento, il cui Direttore, una volta concessa la propria autorizzazione, la inoltrerà alla Direzione Generale dell'Azienda Ospedaliera, la quale esaminerà la richiesta, avvalendosi dei collaboratori che riterrà opportuno (compreso un eventuale parere del DPO). Nel caso la Direzione riterrà coerente e nell'interesse dell'Azienda quanto richiesto, rilascerà il proprio nulla osta. La segreteria della Direzione Generale inoltrerà la pratica al SITAD. Il Responsabile SITAD apporrà il proprio visto e assegnerà la pratica ad uno dei tecnici per procedere con la configurazione e supporto al fornitore.



8. Modifica VPN

La modifica di una VPN può avvenire a seguito di:

- variazione dei riferimenti ai quali è associata la VPN,
- ampliamento/rimozione delle utenze terze parti associate ad una VPN,
- variazione dei sistemi/dati ai quali si accede tramite la VPN,
- Prolungamento temporale della connessione VPN

La modifica può essere richiesta direttamente alla segreteria del SITAD o della Direzione. Se si tratta solo di cambio dei nominativi o della tecnologia di connessione, configurerà direttamente, se invece si chiede il prolungamento rispetto al termine stimato, chiederà gli opportuni pareri prima di procedere.

Di norma, per tutte le attività legate a contratti di manutenzione annuale, il collegamento VPN ha validità annuale; al termine del periodo, sarà cura del soggetto intestatario della VPN chiederne il rinnovo. Per tutto il resto delle attività, la durata deve essere specificata dal richiedente e sottoposta al vaglio dell'Azienda Ospedaliera.

9. Disattivazione VPN

La disattivazione di una VPN può avvenire a seguito di richiesta da parte dei riferimenti indicati nei moduli di richiesta, quando vengano meno le motivazioni per la sua esistenza.

La richiesta va indirizzata alla segreteria del SITAD, che la inoltrerà al Responsabile del SITAD il quale, apposto il proprio visto, la assegnerà al tecnico che effettuerà la disattivazione.

10. Monitoraggio VPN

Il monitoraggio, eseguito tramite il software la lettura dei log di accesso, ha l'obiettivo di verificare l'allineamento tra quanto autorizzato e quanto realmente configurato nei dispositivi abilitanti le VPN. Il Responsabile del SITAD, o un suo delegato, accedendo al software di monitoraggio possono verificare quali utenti si sono collegati alla VPN, gli orari di connessione, la durata e i server o i database ai quali hanno avuto accesso.

I controlli vengono fatti a campione o dietro particolari condizioni di alert configurate dal software stesso (ad. Es. troppe connessioni contemporanee, comportamenti anomali, tentativi di accedere a macchine non autorizzate).

Qualora l'utente stesso o altro soggetto abbia necessità di richiedere informazioni sui collegamenti effettuati o abbia necessità di controllare i log, dovrà inoltrare una richiesta in tal senso alla Direzione Aziendale che, se riterrà la richiesta pertinente, provvederà a inoltrarla al Responsabile SITAD per il seguito di competenza.

Allegato 1
Modulo richiesta accesso remoto per dipendenti

Nome e Cognome del richiedente: _____

Codice Fiscale: _____

E-mail: _____

Tipologia di contratto: ☐ **Amministrativo** ☐ **Sanitario**

Altro (specificare): _____

Durata dell'accesso richiesto: _____

Indicare le applicazioni o i server aziendali per i quali si richiede l'accesso tramite VPN:

Server/applicazioni/dispositivi	*Indirizzo IP*	*Porte*

Con la sottoscrizione del presente modulo si conferma che:

- Il richiedente è in possesso delle capacità necessarie per operare sui sistemi informatici elencati e è a conoscenza delle regole di sicurezza, della normativa sulla riservatezza dei dati personali e del Disciplinare Aziendale sul corretto utilizzo dei dispositivi informatici, telematici, Internet e posta elettronica.
- Il codice di accesso e la relativa password sono personali e non saranno cedute a terzi.
- L'uso del codice di accesso è consentito solo per attività relative a quanto esplicitamente richiesto.
- Il titolare dell'accesso è responsabile per ogni azione compiuta utilizzando l'accesso stesso.
- Ogni abuso dell'accesso comporterà l'immediata sospensione delle credenziali.

Data: ____ / ____ /_____

Il richiedente

_____

Il Direttore della S.C.

_____

Compilazione riservata Azienda Ospedaliera

Autorizzazione del Direttore Sanitario (solo per i dipendenti di Area Sanitaria):

Firma: _____

Autorizzazione del Direttore Amministrativo (solo per i dipendenti di Area Amministrativa):

Firma: _____

Visto del Responsabile dei Sistemi Informatici e Transizione all'Amministrazione Digitale:

Firma: _____

Configurazione VPN eseguita in data: _____

Eventuali note:

Firma del tecnico che ha eseguito la configurazione: _____

Allegato 2
Modulo richiesta accesso remoto per fornitori software esterni

Azienda: _____

Nome del software o progetto: _____

Estremi del contratto di manutenzione o delibera di rinnovo: _____

Data di scadenza del contratto. ____ / ____ /____

Indicare i dati degli operatori per i quali si richiede l'accesso ai server/applicazioni aziendali tramite VPN:

cognome	***nome***	***codice fiscale***	***Applicativo o dispositivo***
Email			
Email			
Email			

Se l'Azienda è dotata di un sistema di tracciatura interno, allegare alla presente la relativa documentazione

Server/applicazioni/dispositivi	***Indirizzo IP***	***Porte***

Con la sottoscrizione del presente modulo si conferma che:

- I tecnici elencati sono in possesso delle capacità necessarie per operare sui sistemi informatici elencati e sono stati opportunamente formati al rispetto delle regole di sicurezza e della normativa sulla riservatezza dei dati personali.
- Il codice di accesso e la relativa password sono personali e non saranno cedute a terzi.
- L'uso del codice di accesso è consentito solo per attività relative al contratto indicato.
- Il titolare dell'accesso è responsabile per ogni azione compiuta utilizzando l'accesso stesso.
- Ogni abuso dell'accesso comporterà l'immediata sospensione delle credenziali.

Data: ____ / ____ /_____

Il legale rappresentante

_____

Compilazione riservata Azienda Ospedaliera

Autorizzazione del Direttore esecutivo del contratto o responsabile della S.C. di riferimento (obbligatoria se nel contratto non sono specificate le modalità di assistenza remota):

Cognome/nome e ruolo _____

Firma: _____

Visto del Responsabile dei Sistemi Informatici e Transizione all'Amministrazione Digitale:

Firma: _____

Configurazione VPN eseguita in data: _____

Eventuali note:

Firma del tecnico che ha eseguito la configurazione: _____

Allegato 3
Modulo richiesta accesso remoto per fornitori di dispositivi elettromedicali e software correlati

Azienda: _____

Contratto di fornitura/servizio: _____

Tipologia di dispositivo o software correlato: _____

Estremi del contratto di manutenzione o delibera di rinnovo: _____

Data di scadenza del contratto. ____ / ____ /____

Indicare i dati degli operatori per i quali si richiede l'accesso ai server/applicazioni aziendali tramite VPN:

cognome	***nome***	***codice fiscale***	***Applicativo o dispositivo***
Email			
Email			

Se l'Azienda è dotata di un sistema di tracciatura interno, allegare alla presente la relativa documentazione

Server/applicazioni/dispositivi	***Indirizzo IP***	***Porte***

Con la sottoscrizione del presente modulo si conferma che:
- I tecnici elencati sono in possesso delle capacità necessarie per operare sui sistemi informatici elencati e sono stati opportunamente formati al rispetto delle regole di sicurezza e della normativa sulla riservatezza dei dati personali.
- Il codice di accesso e la relativa password sono personali e non saranno cedute a terzi.
- L'uso del codice di accesso è consentito solo per attività relative al contratto indicato.
- Il titolare dell'accesso è responsabile per ogni azione compiuta utilizzando l'accesso stesso.
- Ogni abuso dell'accesso comporterà l'immediata sospensione delle credenziali.

Data: ____ / ____ /_____

Il legale rappresentante

_____

Compilazione riservata Azienda Ospedaliera

Autorizzazione del Direttore della S.C. Bioingeneria

Firma: _____

Visto del Responsabile dei Sistemi Informatici e Transizione all'Amministrazione Digitale:

Firma: _____

Configurazione VPN eseguita in data: _____

Eventuali note:

Firma del tecnico che ha eseguito la configurazione: _____

Allegato 4
Modulo richiesta accesso remoto per soggetti esterni senza rapporti contrattuali con l'Azienda

Nominativo del richiedente: _____

Ente o Azienda di appartenenza: _____

Motivo della richiesta: _____

_____

_____

Durata del collegamento richiesto: _____

Indicare i server/applicazioni aziendali tramite VPN:

Server/applicazioni/dispositivi	*Indirizzo IP*	*Porte*

Con la sottoscrizione del presente modulo si conferma che:
- Il richiedente è in possesso delle capacità necessarie per operare sui sistemi informatici elencati e sono stati opportunamente formati al rispetto delle regole di sicurezza e della normativa sulla riservatezza dei dati personali.
- Il codice di accesso e la relativa password sono personali e non saranno cedute a terzi.
- L'uso del codice di accesso è consentito solo per attività relative al contratto indicato.
- Il titolare dell'accesso è responsabile per ogni azione compiuta utilizzando l'accesso stesso.
- Ogni abuso dell'accesso comporterà l'immediata sospensione delle credenziali.

Data: ____ / ____ /_____

Il legale rappresentante

_____

Compilazione riservata Azienda Ospedaliera

Autorizzazione del Direttore della S.C. di riferimento:

Cognome/nome e ruolo _____

Firma: _____

Nulla osta del Direttore Generale:

Firma: _____

Visto del Responsabile dei Sistemi Informatici e Transizione all'Amministrazione Digitale:

Firma: _____

Configurazione VPN eseguita in data: _____

Eventuali note:

Firma del tecnico che ha eseguito la configurazione: _____

Stemma dell'Ospedale di S. Maria della Misericordia di Perugia

Azienda Ospedaliera di Perugia

Dir. Gen. e Sede Amm.va: Piazzale G. Menghini n. 8/9- 06129 PERUGIA
Sede Legale: S. Maria della Misericordia in S. Andrea delle Fratte 06156PERUGIA
Partita IVA 02101050546 Tel. 075 5781 - Sito Internet: www.ospedale.perugia.it

UFFICIO DELIBERAZIONI

ATTESTAZIONI RELATIVE ALLA DELIBERA N. 1011 **DEL** - 7 NOV. 2019

La deliberazione sopra indicata, alla quale questo documento è allegato

CONSTA DI FOGLI 22 incluso il presente ed inclusi gli allegati

Perugia, - 7 NOV. 2019

IL RESPONSABILE DEL PROCEDIMENTO DELIBERATIVO
DOTT.SSA MARIA CRISTINA CONTE

☒ E' ESECUTIVA IMMEDIATAMENTE, non essendo soggetta a controllo

☐ HA CONSEGUITO ESECUTIVITA' IL _____

☐ PER PROVVEDIMENTO POSITIVO DELLA GIUNTA REGIONALE N. _____ DEL _____

CHE HA RICEVUTO LA DELIBERA IL _____

☐ PER DECORRENZA DEL TERMINE DI LEGGE PER IL CONTROLLO SENZA RILIEVI DA PARTE DELLA GIUNTA REGIONALE, CHE HA RICEVUTO LA DELIBERA IL _____

☐ ALTRO (esecutività dopo richiesta di chiarimenti, parziale annullamento dell'atto, annullamento integrale, ecc.. – Specificare gli estremi dei provvedimenti)

Perugia, - 7 NOV. 2019

IL RESPONSABILE DEL PROCEDIMENTO DELIBERATIVO
DOTT.SSA MARIA CRISTINA CONTE

La deliberazione sopra indicata, alla quale questo documento è allegato,

VIENE PUBBLICATA all'albo pretorio dell'Azienda Ospedaliera di Perugia il - 7 NOV. 2019

per la durata di 15 giorni.

Perugia, - 7 NOV. 2019

IL RESPONSABILE DEL PROCEDIMENTO DELIBERATIVO
DOTT.SSA MARIA CRISTINA CONTE

Questa copia della delibera sopra indicata è conforme al suo originale esistente presso questo ufficio e consta di n. _____ pagine inclusa la presente

Perugia,

IL RESPONSABILE DEL PROCEDIMENTO DELIBERATIVO
DOTT.SSA MARIA CRISTINA CONTE