S.C. INFORMATICA E TELECOMUNICAZIONI - 1114 REG.DEC.

OGGETTO: Approvazione del Regolamento per l'utilizzo delle risorse informatiche e telematiche

SERVIZIO SANITARIO REGIONALE
AZIENDA SANITARIA UNIVERSITARIA
GIULIANO ISONTINA

DECRETO
DEL DIRETTORE GENERALE

L'anno **duemilaventuno**
il giorno ventiquattro del mese di DICEMBRE

IL DIRETTORE GENERALE

dott. Antonio Poggiana

nominato con Delibera della Giunta Regionale n° 2266 dd. 27 dicembre 2019

OGGETTO: Approvazione del Regolamento per l'utilizzo delle risorse informatiche e telematiche

Premesso che l'Azienda Sanitaria Universitaria Giuliano Isontina (ASUGI) nello svolgimento della propria attività istituzionale, impiega le risorse ad essa assegnate secondo criteri di efficienza, efficacia ed economicità, mediante l'utilizzo appropriato e corretto delle risorse informatiche e telematiche;

considerato che l'Azienda provvede all'organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche informatici, che facilitano l'accesso e la fruizione delle informazioni;

visto l'art.3 bis della L.241/1990, il quale prevede che le pubbliche amministrazioni agiscano mediante strumenti informatici e telematici sia nei rapporti interni che esterni, al fine di conseguire maggiore efficienza nella loro attività,

visto il Regolamento Generale sulla Protezione dei Dati (RGPD, Regolamento UE 2016/679);

visto il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 (Decreto Legislativo 196/2003 e ss.mm.ii.);

viste le Linee Guida ed i provvedimenti della Autorità Garante per la Protezione dei Dati Personali;

vista la Circolare 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" dell'Agenzia per l'Italia Digitale (AgID);

visto il Piano triennale 2020-2022 per l'informatica nella Pubblica Amministrazione dell'Agenzia per l'Italia Digitale (AgID);

visto il D.Lgs. 518/1992 *Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore*;

vista la L. 248/2000 *Nuove norme di tutela del diritto di autore*;

evidenziato inoltre che la rete aziendale, essendo intrinsecamente una rete IT medicale secondo la norma ISO IEC 80001-1 (*Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software*), è progettata e realizzata con il fine di perseguire l'aderenza ai dettami di questa norma di settore ed in particolar modo alle sue proprietà chiave di sicurezza fisica (delle persone), efficacia, sicurezza dei dati e dei sistemi;

rilevato dunque che è necessario impartire delle regole per operare nell'ottica di mantenere i rischi residui legati alla minaccia cibernetica e ai trattamenti dei dati a livelli accettabili ed evitare, quindi, l'uso improprio o poco consapevole delle risorse informatiche e telematiche e dei dati, ciò al fine di perseguire la cyber security, proteggere le risorse e i dati nonché garantirne riservatezza, integrità e disponibilità nel rispetto di quanto previsto dalla normativa sopracitata;

visto il decreto n.649 dd 30.07.2021 con il quale questa Azienda ha approvato il documento "Budget 2021 – Piano Complessivo Aziendale" – costituente il quadro degli obiettivi incentivanti assegnati ai Centri di Responsabilità aziendali;

evidenziato che, tra gli obiettivi incentivanti attribuiti alla S.C. Informatica e Telecomunicazioni per l'anno 2021, vi è la presentazione del regolamento per l'utilizzo delle risorse informatiche e telematiche;

considerato che, per effetto del combinato disposto dell'art.11 della L.R. 27/2018 e della D.G.R. 2174 dd. 12.12.2019, sono state soppresse le precedenti aziende Azienda per l'Assistenza Sanitaria n.2 (ASS2) e Azienda Sanitaria Universitaria Integrata di Trieste (ASUITS) ed è stata costituita la nuova Azienda Sanitaria Universitaria Giuliano Isontina (ASUGI) a decorrere dal 01.01.2020, che subentra in tutti i rapporti giuridici attivi e passivi delle soppresse Aziende;

visto che già l'allora Azienda Ospedaliero-Universitaria "Ospedali Riuniti di Trieste" (AOUTS) era dotata di un regolamento aziendale sull'utilizzo delle risorse informatiche, come modificato da ultimo con Delibera n.407 dd.11 dicembre 2014;

che già AAS2 aveva predisposto una procedura aziendale per il trattamento dei dati ed un documento programmatico sulla sicurezza, con quota parte di contenuti relativi all'utilizzo delle risorse informatiche, come da decreto AAS2 n. 276 dd. 3 giugno 2016;

precisato che il regolamento per l'utilizzo delle risorse informatiche e telematiche è stato predisposto dalla SC Informatica e Telecomunicazioni anche tenendo conto di quanto contenuto nei precedenti regolamenti ma aggiornandone i contenuti, considerata l'evoluzione tecnologica dei sistemi IT;

considerato che, per i motivi sin qui esposti, l'Azienda intende procedere all'adozione del regolamento di cui sopra, anche al fine di superare le diverse regolamentazioni attualmente vigenti;

che il regolamento entrerà in vigore alla data di approvazione con decorrenza *ex nunc*, senza assumere efficacia retroattiva;

rilevato che il provvedimento è proposto dal Direttore della S.C. INFORMATICA E TELECOMUNICAZIONI, che attesta la regolarità tecnica, amministrativa e la legittimità dell'atto e i cui uffici ne hanno curato l'istruzione e la redazione;

acquisito il parere favorevole del Direttore Sanitario, del Direttore Amministrativo e del Direttore dei Servizi Sociosanitari;

IL DIRETTORE GENERALE

DECRETA

per quanto esposto in narrativa:

- di approvare il Regolamento per l'utilizzo delle risorse informatiche e telematiche, allegato al presente provvedimento quale parte integrante dello stesso.

Nessuna spesa consegue all'adozione del presente provvedimento che diviene esecutivo, ai sensi dell'art. 4 della L.R. 21/92, dalla data di pubblicazione all'Albo aziendale telematico.

IL DIRETTORE GENERALE
dott. Antonio Poggiana

Parere favorevole del Direttore Sanitario dott. Andrea Longanesi	Parere favorevole del Direttore Amministrativo dott. Eugenio Possamai	Parere favorevole del Direttore dei Servizi Sociosanitari dott. Fabio Samani

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: ANDREA LONGANESI
CODICE FISCALE: LNGNDR61R19A547T
DATA FIRMA: 24/12/2021 14:27:38
IMPRONTA: 2B012EBC9A37C2E1A0901BCADD92D270827101AD4333BB814ECB95DBF93FDA54
827101AD4333BB814ECB95DBF93FDA54B1CE166E3D7FE65D4452A2F269F39369
B1CE166E3D7FE65D4452A2F269F393693C013CF9ABE4FCB6674EB39CD34FEF91
3C013CF9ABE4FCB6674EB39CD34FEF91A458EB9E183A8CE0CB5BDB7EA30148EF

NOME: EUGENIO POSSAMAI
CODICE FISCALE: PSSGNE59M27C957L
DATA FIRMA: 24/12/2021 15:02:58
IMPRONTA: 8E957492DC34437ACCA8ED66DFD9B98C074B0C11E22CCD289D1E56576970A497
074B0C11E22CCD289D1E56576970A4977A43F3729D08AC321255D51712ADC8D3
7A43F3729D08AC321255D51712ADC8D36C2B359AEC8A29E2670192EA26E38741
6C2B359AEC8A29E2670192EA26E387412BC1F857A7315AB7D30311A9956AC667

NOME: ANTONIO POGGIANA
CODICE FISCALE: PGGNTN64M30C743F
DATA FIRMA: 24/12/2021 15:35:56
IMPRONTA: 44C365093192A084ECA871B5393333FA352FAA4550E8274310C53E5AD1C70D5C
352FAA4550E8274310C53E5AD1C70D5C9105240BD73A679D9E090755E4CF625D
9105240BD73A679D9E090755E4CF625D3CCF2A0284F597AA9EE0795B632CD81D
3CCF2A0284F597AA9EE0795B632CD81D250B92EC0A831C433D593EC183A6E415

NOME: FABIO SAMANI
CODICE FISCALE: SMNFBA57C03L424I
DATA FIRMA: 24/12/2021 16:55:18
IMPRONTA: 5288B84A4BC76DE7E2F25213C0D4245B759189CC3D1DA458990C4B3E0103E032
759189CC3D1DA458990C4B3E0103E03286F28DEF75E6B98304489174177783D47
86F28DEF75E6B98304489174177783D47A15A76B6FA48231E01C7DAAE19BA0E5E
A15A76B6FA48231E01C7DAAE19BA0E5E8641F75C638B07385D63E00BBDE8F116

REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE

MATRICE DELLE REVISIONI					
REVISIONE	DATA	DESCRIZIONE	REDAZIONE	VERIFICATA	APPROVATA
00	15/12/2021	1a emissione		SCIT	DA

INDICE

ART. 1 SCOPO E FINALITÀ

Questo documento raccoglie le principali regole di comportamento che devono essere adottate nell'utilizzo delle risorse informatiche e telematiche messe a disposizione dall'Azienda Sanitaria Universitaria Giuliano Isontina (di seguito denominata ASUGI o Azienda) per l'attività lavorativa.
Nella sfera delle risorse informatiche e telematiche ASUGI, in via non esclusiva, rientrano: Personal Computer (PC) fissi e portatili, dispositivi mobili (cellulari e tablet), sistemi di stampa e scanner locali o di rete, periferiche varie (monitor, mouse, tastiere, webcam, microfoni), dispositivi di archiviazione (dischi esterni, pendrive USB, CD, DVD), sistemi di connettività dati (cablati e wireless), telefoni fissi e cordless, fax, dispositivi cercapersona; inoltre programmi e applicativi nonché le relative basi di dati (DB) tra cui il directory service aziendale (dominio AD), la posta elettronica aziendale, gli applicativi di base (pacchetto office, software di firma digitale, web browser, etc), gli applicativi specialistici sanitari, tecnici ed amministrativi.

L'obiettivo primario del presente Regolamento è impartire delle regole per operare nell'ottica di mantenere i rischi residui legati alla minaccia cibernetica e ai trattamenti dei dati a livelli accettabili ed evitare, quindi, l'uso improprio o poco consapevole delle risorse informatiche e telematiche e dei dati, nonché innalzare la percezione di pericolo e di reato. Ciò nell'ottica di perseguire la cyber security, proteggere le risorse e i dati e garantirne riservatezza, integrità e disponibilità nel rispetto di quanto previsto in particolare da: il Regolamento Generale sulla Protezione dei Dati (RGPD, Regolamento UE 2016/679), il Codice in Materia di Protezione dei Dati Personali (Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.); le Linee Guida e i Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali; l'Agenzia per l'Italia Digitale (AgID) con particolare attenzione alla Circolare 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni"; le leggi sul diritto d'autore (D.Lgs. 518/1992 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore" e L. 248/2000 "Nuove norme di tutela del diritto di autore"); le norme di settore e le best practice. Si evidenzia inoltre che la rete aziendale, essendo intrinsecamente una rete IT medicale secondo la norma IEC 80001-1, è progettata e realizzata con il fine di perseguire l'aderenza ai dettami di questa norma di settore ed in particolar modo alle sue proprietà chiave di sicurezza fisica (delle persone), efficacia, sicurezza dei dati e dei sistemi.

Il secondo obiettivo è quello di chiarire alcuni aspetti fondamentali relativi alle modalità e alle clausole di utilizzo delle risorse informatiche e telematiche, al fine di:

- regolamentarne l'utilizzo in modo che siano utilizzate in maniera efficiente, efficace, produttiva ed orientata al raggiungimento degli obiettivi aziendali;
- garantire, salvaguardare e tutelare ASUGI ed il personale autorizzato durante l'utilizzo delle risorse informatiche e telematiche anche in considerazione di rischi di natura patrimoniale;
- prevenire l'uso improprio delle risorse informatiche e telematiche e garantire la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi;
- regolamentare in particolare l'utilizzo dei dispositivi mobili e dei supporti esterni di memorizzazione, della navigazione in internet e della posta elettronica.
- accrescere le competenze in ambito digitale e promuovere la trasformazione digitale della pubblica amministrazione e dei suoi dipendenti in ottica di semplificazione e di miglioramento dell'efficienza, in linea con gli indirizzi nazionali del Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022.

Nella redazione del Regolamento si è quindi tenuto conto di quanto segue:

- l'utilizzo delle risorse informatiche e telematiche, come quello di qualsiasi bene aziendale, deve sempre ispirarsi ai principi di diligenza e correttezza impliciti nell'ambito del rapporto di lavoro all'interno della Pubblica Amministrazione (PA);
- ogni trattamento di dati personali e di categorie particolari di dati personali[1] (precedentemente denominati "sensibili") deve essere lecito, pertinente e non eccedente, e non devono mai essere posti in essere trattamenti che possano in qualunque modo inficiare riservatezza, integrità e disponibilità (acronimo RID) anche in riferimento al know how aziendale.

La stesura del presente regolamento è stata effettuata a cura della Struttura Complessa Informatica e Telecomunicazioni (SCIT) che per mandato aziendale gestisce le risorse informatiche e telematiche aziendali, di concerto con il Responsabile Protezione Dati di ASUGI (RPD/DPO), secondo gli indirizzi della Direzione Strategica.
È inoltre affidato alla SCIT il compito di effettuare il monitoraggio del patrimonio ICT aziendale al fine di garantirne la continuità di servizio e la sicurezza, anche con verifiche a campione e a seguito di qualunque anomalia o segnalazione, nel rispetto del presente regolamento.

ART. 2 AMBITO DI APPLICAZIONE

Questo regolamento si applica:

a) a tutti i soggetti che utilizzano le risorse informatiche messe a disposizione da ASUGI;
b) a tutti i soggetti autorizzati al trattamento dati[2], dipendenti e non, nel seguito anche utenti, ovvero a tutti coloro in possesso di credenziali di accesso alle risorse informatiche e telematiche di ASUGI;
c) a tutte le risorse informatiche e telematiche di ASUGI o comunque messe a disposizione da ASUGI, compresi i sistemi di comunicazione e trasmissione dati mobili;
d) a tutte le forme di comunicazione interna ed esterna operate attraverso Internet, posta elettronica e ogni altro sistema telematico di comunicazione dei dati di titolarità o responsabilità di ASUGI;
e) all'utilizzo di tutti i tipi di supporti di memorizzazione di dati, audio e video, analogici e digitali, dedicati e non dedicati, a qualunque titolo utilizzati all'interno di ASUGI e destinati all'archiviazione di dati, documenti informatici, registrazioni.

Ciascun soggetto utilizzatore e/o autorizzato in ASUGI deve attenersi a quanto qui regolamentato.
Tutto quanto non espressamente permesso si intende in generale vietato.
Il mancato rispetto delle regole impartite da ASUGI al riguardo comporta l'assunzione diretta da parte dei soggetti incaricati di responsabilità nascenti da tali condotte e determina, nei casi ed entro i limiti previsti dalla normativa vigente, la contestabilità: anche qualora non si configuri direttamente un reato, potrà essere comunque intentato un procedimento disciplinare e risarcitorio.

ART. 3 ACRONIMI E DEFINIZIONI

CO – Carta Operatore
CRS – Carta Regionale dei Servizi (detta tessera sanitaria)

[1] Inerenti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

[2] Autorizzato al trattamento dei dati (A-TD) è chiunque abbia ricevuto da un Direttore di Struttura Complessa, di Distretto, di Dipartimento o di Direzione Strategica, una specifica autorizzazione al trattamento dei dati e la relativa formazione in materia, e può quindi effettuare trattamenti di titolarità ASUGI. Gli A-TD corrispondono agli "incaricati" secondo la pre-esistente normativa.

Dir-TD – Direttore Trattamento Dati
DPO – Data Protection Officer (uguale a RPD – Responsabile Protezione Dati)
PC – Personal Computer
RFID – Radio Frequency Identification
RID – Riservatezza, Integrità e Disponibilità
RPD – Responsabile Protezione Dati
SCIT – SC Informatica e Telecomunicazioni
SISSR – Sistema Informativo Socio Sanitario Regionale

ART. 4 RIFERIMENTI NORMATIVI

Regolamento Generale sulla Protezione dei Dati (RGPD, Regolamento UE 2016/679);
Codice in Materia di Protezione dei Dati Personali (Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.);
Linee Guida e Provvedimenti della Autorità Garante per la Protezione dei Dati Personali;
Circolare 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" dell'Agenzia per l'Italia Digitale (AgID);
Piano triennale 2020-2022 per l'informatica nella Pubblica Amministrazione dell'Agenzia per l'Italia Digitale (AgID);
D.Lgs. 518/1992 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore";
L. 248/2000 "Nuove norme di tutela del diritto di autore";
Norma ISO IEC 80001-1:2021Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software — Part 1: Application of risk management.

ART. 5 REGOLE GENERALI RELATIVAMENTE ALLE RISORSE INFORMATICHE E TELEMATICHE AZIENDALI

Le risorse informatiche e telematiche vengono assegnate su richiesta dei Direttori di Struttura Complessa, di Distretto, di Dipartimento e dei Direttori della Direzione Strategica (di seguito in breve solo struttura) e devono essere custodite con cura ed utilizzate nel modo previsto, evitando manomissioni, danneggiamenti o comunque utilizzi non consentiti.
In caso di trasferimento di ufficio o di funzione, tutte le risorse informatiche e telematiche restano in carico alla struttura, salvo esplicita autorizzazione da parte del Direttore della struttura, il quale provvederà anche al passaggio in carico d'inventario. Non è comunque consentito lo spostamento in autonomia di telefoni, PC e relative periferiche.
È compito della SCIT valutare lo stato di obsolescenza del materiale affidato e prevedere dei piani di sostituzione dello stesso.

Le risorse informatiche e telematiche, siano esse condivise o affidate alla singola persona, sono strumenti di lavoro in custodia e sotto la responsabilità di ciascuno e del Direttore della struttura, appartenenti al patrimonio aziendale, e pertanto come tali vanno utilizzati e vanno custoditi in modo appropriato. I dispositivi mobili e quelli portatili non devono mai essere lasciati incustoditi.
Il furto, il danneggiamento o lo smarrimento di un dispositivo deve essere prontamente denunciato alle autorità competenti e la denuncia deve essere inviata al protocollo generale di ASUGI e per conoscenza alla SCIT.

Tutte le risorse informatiche e telematiche vanno utilizzate in modo attento e consapevole in quanto ogni loro utilizzo disattento o inconsapevole può contribuire a provocare disservizi, aumentare i costi di manutenzione e creare potenziali minacce alla sicurezza dell'infrastruttura informatica (di seguito solo IT) e dei dati sia dell'Azienda sia di tutto il Sistema Informativo Socio Sanitario Regionale (SISSR).

Le dotazioni IT aziendali vengono consegnate con adeguata configurazione hardware e software. Anche ove tecnicamente possibile, è vietato modificare sia la configurazione hardware che software. Questo comprende, tra l'altro, il divieto di installare periferiche anche USB e di utilizzare software non autorizzati.

La rete dati ASUGI garantisce la connettività delle attrezzature aziendali autorizzate. È vietato collegare in rete dispositivi non autorizzati da SCIT. Ove disponibile è possibile collegare dispositivi personali alla rete "Guest".

L'ASUGI adotta ogni misura ritenuta necessaria al fine della riduzione dei consumi di materiali ed energia. In linea con tale condotta, va minimizzato il ricorso alla stampa ed in generale l'uso di materiale di consumo e, al termine dell'orario di lavoro, l'utente deve provvedere allo spegnimento di ogni risorsa informatica che non è necessario rimanga accesa: i monitor vanno sempre spenti e le stampanti di rete vanno poste in modalità di risparmio energetico. Nel caso in cui la postazione debba rimanere accesa è necessario disconnettersi o bloccare la sessione di lavoro (così come ogni volta in cui ci si allontana dalla postazione in uso).

ART. 6 TRATTAMENTO DI DATI PERSONALI E DI CATEGORIE PARTICOLARI (EX SENSIBILI) MEDIANTE RISORSE INFORMATICHE E TELEMATICHE ASUGI

Qualunque trattamento di dati personali deve essere lecito e svolto secondo quanto previsto dalla normativa vigente sull'argomento.
I dati aziendali, personali e appartenenti a categorie particolari, così come i dati giudiziari, vanno minimizzati e trattati mantenendoli protetti da rischi di perdita di riservatezza, integrità e disponibilità.
I dati vanno trattati solo negli applicativi a ciò deputati, da cui – in quota parte ritenuta regionalmente e/o aziendalmente necessaria – conservati a norma di legge per il tempo previsto dal manuale della conservazione, ovvero nelle modalità previste nel presente regolamento.
Al di fuori di tali applicativi, vanno archiviati solo i dati necessari, pertinenti e non eccedenti, e solo per il tempo strettamente necessario, con riferimento allo scopo dello specifico trattamento, effettuato al di fuori degli applicativi aziendali di cui sopra. In generale va quindi privilegiata la "minimizzazione" dei dati ed è responsabilità e cura del Dir-TD[3] la corretta gestione degli archivi e la relativa cancellazione dei dati non più necessari.
Sui PC, e in generale su qualunque dispositivo aziendale, non devono essere archiviati dati personali, giudiziari, e di categorie particolari. Questo significa che i dischi locali non possono configurarsi come archivi di dati particolari (repository); infatti per esempio i dischi dei normali PC aziendali non sono soggetti ad alcun tipo di backup, cioè del contenuto di questi dischi non vengono eseguite copie di sicurezza e nel caso di fisiologica rottura del disco tutti i dati in esso contenuti vanno irrimediabilmente persi; inoltre, generalmente, la sicurezza fisica dei PC aziendali non può essere garantita in quanto di facile accessibilità e, quindi, considerato che i dati locali perlopiù non sono cifrati, possono essere carpiti a seguito del furto fisico del disco rigido stesso. Possono essere salvati dati di altra natura nelle more di quanto sopra riportato, ossia dati la cui perdita non crea disservizio.
I dati aziendali, personali, giudiziari e particolari in generale non devono essere salvati su alcun dispositivo rimovibile (pendrive, disco rigido esterno, CD, DVD, ecc.) o mobile (PC portatile, phablet, tablet, smartphone, ecc.) a meno che non siano crittografati in maniera sufficientemente robusta.
I dati personali e particolari, tra cui sensibili (esclusi i dati genetici e biometrici), possono essere inviati tramite casella di posta elettronica ordinaria (PEO) aziendale solo in caso di stretta necessità e

[3] Sono "Direttore del Trattamento Dati" il Direttore Amministrativo, il Direttore Sanitario, il Direttore Sociosanitario, i Direttori di Distretto, di Dipartimento e di Struttura Complessa.

solo in forma di allegato, ovvero non come testo del messaggio. Il file allegato dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni da parte di soggetti diversi da quelli autorizzati. Potrà consistere in algoritmo di cifratura a singola chiave (ovvero in un file cifrato protetto da password per l'apertura; in tal caso sia algoritmo che password dovranno essere opportunamente robusti) o in un algoritmo di cifratura a doppia chiave asimmetrica (ad esempio cifratura tramite la carta di firma digitale); ma in ogni caso le chiavi di decifratura dovranno essere rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione del file. Buona pratica poi la cancellazione della email appena possibile.

È permesso inviare dati personali e particolari, tra cui sensibili (esclusi i dati genetici e biometrici), tramite casella di Posta Elettronica Certificata (PEC) aziendale, alla casella PEC dei soli interessati (proprietari del dato) che abbiano espressamente prestato il consenso oppure alla casella PEC di soggetti istituzionali terzi con i quali sia contrattualizzato un esplicito accordo di responsabilità.
In generale l'uso del fax da e verso l'esterno di ASUGI è vietato. Va prestata la massima attenzione nell'inviare dati sensibili via fax all'interno di ASUGI: va utilizzato tale strumento (tecnologicamente obsoleto ed in via di dismissione a livello nazionale) solo per i flussi aziendali residuali che non abbiano alcuna possibilità di trasmissione nell'ambito di un applicativo o in modalità cartacea, controllando in ogni caso scrupolosamente il numero di destinazione e la corretta presa in carico da parte del destinatario.
Analogamente, va prestata la massima attenzione nel non diffondere dati personali, giudiziari e sensibili via stampanti di rete (stampanti o fotocopiatrici) per evitare che la stampa possa essere visionata da non autorizzati: va controllata scrupolosamente la correttezza del nome della stampante di rete prima di inviare il documento in stampa. Il materiale stampato deve essere immediatamente prelevato per evitare che possa essere visionato da personale non autorizzato.
La funzione "scan to mail" delle fotocopiatrici multifunzione collegate in rete deve essere utilizzata solamente verso l'indirizzo e-mail dell'operatore che effettua la scansione che provvederà all'eventuale inoltro alla persona interessata. Considerato che il canale di invio non è crittografato, per questa fattispecie si rimanda al paragrafo di cui sopra relativo alla PEO.
È vietato esfiltrare dati aziendali, dati personali, giudiziari e sensibili con qualunque mezzo (es. Dropbox, Google Drive, MS Drive, Apple ICloud, Amazon Cloud, WhatsApp, email personali, ecc.) e verso qualunque destinatario, se non aziendalmente contrattualizzato.
Per necessità di scambio dati tra sedi remote e con utenti esterni all'organizzazione, strumento consentito – anche per lo scambio di dati sensibili – è quello da Insiel SpA e denominato "Sc@mbio". Lo strumento consente di creare delle box riservate ed a tempo con cui caricare file (consultabili tramite un link da internet) oppure creare una box su cui terzi possono caricare file dall'esterno. Questo strumento è consentito in quanto l'accesso al servizio avviene con un account/casella di posta aziendale, i dati non vengono salvati su un ambiente cloud, ma su server Insiel, è garantita la protezione dei dati tramite cifratura SSL e la permanenza è temporanea.
Per richiedere l'attivazione fare richiesta tramite canali di assistenza informatica aziendale.

È vietato trattare dati personali, giudiziari e sensibili anche su dispositivi fissi e mobili di proprietà personale.

ART. 7 ACCESSO ALLE RISORSE INFORMATICHE E TELEMATICHE: SISTEMI DI AUTENTICAZIONE

7.1. Credenziali

L'accesso alle risorse informatiche e telematiche aziendali è regolato, in ottemperanza agli obblighi di legge, da "credenziali utente" personali e non cedibili, che devono essere quindi custodite ed utilizzate dagli autorizzati con la massima diligenza e non devono essere divulgate per nessun motivo.

L'assegnazione delle credenziali utente agli autorizzati avviene secondo quanto previsto nel "Regolamento per l'erogazione, l'uso e la dismissione dei permessi di accesso alle banche dati informatizzate centralizzate in uso in ASUGI". Non sono consentite utenze impersonali.

Di seguito si riportano alcune caratteristiche peculiari relative alle credenziali utente di accesso ai Personal Computer (PC) connessi ai domini informatici aziendali (cosiddette "credenziali di dominio"), nonché alcune indicazioni operative relative alla loro gestione.
Tali indicazioni, seppur specifiche per le credenziali di dominio, vanno intese come regola generale d'uso di qualsiasi credenziali di accesso ad una qualsiasi risorsa informatica e telematica.
Si ricorda che l'abuso delle credenziali d'accesso (ossia l'utilizzo per scopi diversi da quelli per cui sono state assegnate), l'accesso alle risorse informatiche con credenziali altrui, la comunicazione ad altri delle proprie password e la loro custodia non adeguata configurano un reato penalmente perseguibile e il trasgressore è soggetto anche a procedimento disciplinare.

Come noto ormai dall'operatività quotidiana, per accedere ad un PC "in dominio", ovvero accedere alla sessione di lavoro individuale di Windows su un PC, è sempre necessario immettere le credenziali di dominio che in ASUGI – oggi – sono così composte:

- "Nome Utente", identificativo associato in modo univoco e definitivo all'utente, tale per cui quando un operatore cessa la sua collaborazione con l'Azienda, il suo nome utente non verrà mai più riutilizzato.
- "Password", rispondente ad alcuni criteri di sicurezza e complessità predefiniti quali:
  - lunghezza minima della password;
  - password history, ossia impedimento di riutilizzare un certo numero di password pregresse;
  - obbligo di utilizzo di almeno una lettera minuscola, una maiuscola ed un numero, oppure un simbolo; blocco all'utilizzo del "nome anagrafico", il "cognome anagrafico" o il "nome utente" dell'operatore;
  - obbligo di cambiare la password al più ogni 90 giorni e vincolo a cambiarla non più di una volta al giorno.
- "Dominio", ossia uno dei domini AD in uso in ASUGI. Infatti nome utente e password sono riferite sempre ad uno specifico dominio.

La complessità imposta per la password viene vanificata se vengono usate parole di dizionario italiano o di altre lingue, se la maiuscola è messa come primo carattere e il numero come ultimo, se l'1 viene usato nelle parole al posto della i e lo 0 al posto della o (la maggior parte delle persone opera in tale maniera ed i sistemi automatici di ricerca password utilizzano queste tecniche).

La password assegnata per il primo accesso al dominio (o tutte le volte che si richiede un reset della password) è una password provvisoria che deve essere obbligatoriamente sostituita al primo accesso dall'autorizzato con una conosciuta soltanto a lui, che dovrà nuovamente sostituire almeno ogni 90 giorni. Nel caso gli utenti sospettino che una propria password abbia perso il requisito di segretezza (e quindi possa essere utilizzata da altri) sono tenuti a sostituirla immediatamente e a darne tempestiva comunicazione al Direttore Trattamento Dati (DIR-TD) della struttura di afferenza.
Da quando la password risulta scaduta (al novantesimo giorno dall'ultimo cambio password) il sistema nega l'accesso all'utente finché lo stesso non avrà provveduto a cambiare con successo la sua password. Quindi la scadenza del periodo di validità della password non comporta mai l'impossibilità per l'utente di accedere ai sistemi.

Le password usate per servizi aziendali non vanno mai utilizzate per altri scopi (sistemi di autenticazione e di accesso di uso personale e domestico, es. email personale) in quanto ciò mette a rischio l'intero ambiente di lavoro e va contro i principi basilari di sicurezza informatica.
Le proprie credenziali non vanno mai digitate su PC non sicuri, ossia su PC che non siano sotto il diretto controllo per gli ambiti di sicurezza di ASUGI o dell'utente (es. Pc di un albergo).

Le credenziali di accesso ai PC in dominio aziendale sono assolutamente personali: identificano in maniera univoca il soggetto autorizzato che ha accesso alle risorse informatiche e legano ad esso tutte le operazioni svolte nel corso della sessione di lavoro di Windows.
Considerato che è via via sempre crescente il numero di risorse informatiche (e-mail aziendale, cartelle condivise, applicativi) cui si accede con le medesime credenziali di dominio, è necessario prestare particolare attenzione a non allontanarsi dal PC con la propria sessione utente attiva (non bisogna cioè "lasciare il PC aperto", come si usa dire): prima di allontanarsi dal PC è obbligatorio "disconnettere l'utente", ovvero chiudere la propria sessione di lavoro[4].
Lasciare un PC incustodito con la sessione di Windows attiva, ovvero non bloccato, può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'uso indebito e configurando comunque il reato di mancata custodia.
È vietata la violazione di qualunque credenziale.
La violazione della password di accensione (di BIOS) dei PC si configura come danneggiamento di bene d'Azienda.

7.2. Altri sistemi di autenticazione

Alcune risorse informatiche consentono l'autenticazione – in alternativa al nome utente e password – tramite mezzi quali la "smart card" - tessera con microchip e PIN numerico, p.e. la Carta Operatore (CO) della Regione FVG o la Carta Regionale dei Servizi (CRS, cosiddetta Tessera Sanitaria) Attiva della Regione FVG – ed il braccialetto contente tag RFID per l'identificazione.
Tali dispositivi devono essere utilizzati e custoditi con la stessa cura e diligenza delle credenziali di accesso (nome utente e password). Gli utenti titolari dei dispositivi sono tenuti ad utilizzare personalmente i dispositivi e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno (p.e. custodire separatamente la smart card dal PIN di attivazione della stessa).
In caso di smarrimento o furto,

- se trattasi di CO, l'utente dovrà richiedere la revoca all'Ufficio di Registrazione ASUGI (istituito nell'ambito della struttura cui compete la gestione del personale); la richiesta dovrà essere sempre corredata dalla denuncia alle autorità di Pubblica Sicurezza.
- se trattasi di CRS Attiva, si rimanda a quanto previsto dalla Regione autonoma Friuli Venezia Giulia.
- se trattasi di braccialetto RFID, l'utente dovrà immediatamente comunicarlo all'Azienda inviando dalla propria e-mail aziendale una e-mail all'indirizzo di posta elettronica certificata PEC di ASUGI e richiedere tempestivamente ai servizi preposti la dissociazione del braccialetto. (Per il corretto utilizzo di questi dispositivi di autenticazione, si rimanda eventualmente anche alle specifiche istruzioni date agli utenti al momento della presa in carico del "dispositivo" stesso.)

Analogamente, sono in corso di validazione sistemi di autenticazione forte aziendali (strong authentication) basati su smart card e PIN (Windows integrated smartcard logon), da gestire come la CO di cui sopra.

[4] Per disconnettere il proprio utente è sufficiente selezionare la voce "Disconnetti" dal menù di avvio di Windows oppure utilizzando da tastiera la combinazione contemporanea di tasti "Ctrl+Alt+Canc – scegliere "disconnetti" e digitare invio. Solo nel caso di PC ad uso esclusivo di un utente, può essere utilizzata la funzione "Blocca" selezionabile dal menù di avvio di Windows, oppure utilizzando da tastiera la combinazione contemporanea di tasti "Ctrl+Alt+Canc" e poi tasto "Invio", o ancora utilizzando da tastiera la combinazione contemporanea di tasti "Windows+L".

ART. 8 UTILIZZO DELLE RISORSE: DIRECTORY SERVICE (DOMINIO) E FILE SERVER

Un "Dominio" è un raggruppamento logico di macchine (PC client e server) e di account (individuali assegnati ad un utente e di servizio utilizzati dalle macchine) che condividono le politiche di sicurezza, le informazioni e le risorse (p.e. cartelle condivise e stampanti).

I PC in dominio aziendale sono un canale di accesso ad altre risorse informatiche centralizzate: gli applicativi (Insiel e non), il fileserver aziendale, la e-mail aziendale, ecc.

Da un dominio aziendale sono accessibili le unità di rete del cosiddetto fileserver: quote di spazio disco su un server centralizzato, ovvero spazio di archiviazione pregiato e ad alto costo, caratterizzato da alta affidabilità intrinseca e soggetto a procedure di backup, per garantire sicurezza e continuità di servizio elevati.
Dal punto di vista delle responsabilità inerenti il trattamento dei dati, quando uno spazio disco è assegnato ad una struttura aziendale (Struttura Complessa, Struttura Semplice Dipartimentale, Distretto, Dipartimento, Direzione), la corretta tenuta dei dati al suo interno è delegata al DIR-TD della struttura stessa. Tale DIR-TD sarà garante, tra l'altro, che quanto in cartella sia pertinente e non eccedente relativamente all'utilizzo previsto, sia dal punto di vista degli utenti a cui viene data visibilità sia dal punto di vista temporale. Sarà inoltre responsabile di organizzare il lavoro in modo tale che nel fileserver non vengano duplicati dati già presenti in altri sistemi aziendali. Premesso che a livello aziendale si ritiene accettabile e sostenibile la tenuta di archivi correnti con orizzonte temporale di cinque anni, SCIT si riserva di cancellare senza ulteriore comunicazione dagli spazi di archiviazione aziendali dati non rispondenti a questa policy. Il file server non è comunque un sistema di conservazione, e va inteso perciò come mero archivio corrente.

La SCIT si riserva di verificare lo stato delle cartelle e richiedere la cancellazione di file nei casi in cui risultino molti file inutilizzati, dimensioni molto elevate delle cartelle o rate di crescita dello spazio occupato molto alti.
Le unità di rete del fileserver sono aree di condivisione di informazioni strettamente professionali e non devono essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere memorizzato, nemmeno per brevi periodi, in queste unità. Anche in quest'ambito, si ribadisce che il trattamento dati deve sempre conformarsi ai principi di minimizzazione, indispensabilità, pertinenza e non eccedenza.
L'Azienda si riserva la facoltà di procedere alla rimozione senza preavviso di qualsiasi file o applicazione memorizzati sulle unità di rete nel caso in cui li ritenga non inerenti l'attività lavorativa o pericolosi per la sicurezza, in violazione di leggi vigenti o regolamenti ovvero che siano stati acquisiti o installati in violazione del presente regolamento.

I dati che si trovano nelle unità di rete del fileserver, se cancellati, non vengono spostati nel cestino ma eliminati in maniera definitiva. In altre parole, la cancellazione di un file da una unità di rete non è un'operazione reversibile in autonomia dall'utente.

L'opportunità dell'utilizzo del fileserver è evidente anche in considerazione del fatto che i dati salvati su uno specifico PC (sia sul disco "C:" o sul disco "D:", che nella cartella "Documenti" o sul "Desktop") sono accessibili solo da quel PC e non sono soggetti a nessuna politica di backup (in caso di rottura del disco rigido i dati vengono persi e non possono essere recuperati in alcun modo).

Per il ripristino dei dati accidentalmente cancellati, persi o modificati sulle cartelle di rete è fatto obbligo di avvisare tempestivamente la SCIT (la retention è limitata, e a lungo termine i dati potrebbero non essere più recuperabili).

In ASUGI sono in uso[5] tre distinti domini aziendali.

8.1. Dominio aouts.it

Gli utenti che utilizzano il dominio aouts.it possono accedere ad un fileserver per l'archiviazione sicura di file e cartelle. La continuità di servizio è garantita dall'alta affidabilità intrinseca del sistema, progettato per garantire nel tempo l'accesso ai dati, con ampi margini sulle fisiologiche rotture dei componenti hardware che lo costituiscono. Tutti i dati archiviati su questo fileserver sono soggetti a specifiche procedure di salvataggio (backup), gestite direttamente dalla SCIT che consentono di recuperare i file cancellati o modificati accidentalmente.

Il fileserver del dominio aouts.it ha una struttura organizzata in un filesystem navigabile dagli utenti e caratterizzato da tre tipologie di cartelle: "Utente", "Reparto", "Misto". Per semplificare l'accesso alle cartelle, in generale, per ciascun utente vengono automaticamente mappate nella sessione di Windows personale - sulla base dei gruppi di dominio di appartenenza - tre specifiche unità di rete denominate dischi (U:), (R:) ed (M:), corrispondenti alle tre tipologie di cartelle di cui sopra, nonché il disco (V:) che consente di navigare ad alto livello tutta la struttura del fileserver e di entrare solo nelle cartelle a cui l'utente è effettivamente abilitato. Tale strutturazione è pensata per rispondere ad esigenze diverse, sia in termini di condivisione di file e archiviazione dati, sia in termini di autorizzazioni necessarie a regolamentarne l'accesso da parte degli utenti di dominio.

L'unita di rete disco (U:) è lo spazio disco del fileserver messo a disposizione di ciascun utente/dipendente, la cui dimensione è limitata. L'accesso avviene dalla sessione di lavoro individuale di ciascun utente da un PC in dominio aouts.it tramite l'icona "Computer" o "Risorse del Computer". I permessi di accesso alle condivisioni utente sono limitati unicamente all'utente stesso ed agli amministratori del dominio. A prescindere dal PC in dominio aouts.it dal quale l'utente lavora, l'unita di rete disco (U:) visualizzata è sempre la stessa: quella personale. La cartella (U:) non viene creata di default, per cui è necessario richiederne l'attivazione tramite i canali di assistenza informatica aziendale. La quantità massima di dati che ogni utente potrà salvare è limitata.

Lo spazio disco del fileserver messo a disposizione di ciascuna struttura aziendale (Struttura Complessa, Struttura Semplice Dipartimentale, Distretto, Dipartimento, Direzione) per la condivisione di file e di cartelle tra gli operatori della struttura stessa è usualmente mappato sul PC con unita di rete disco (R:). L'accesso all'unita di rete disco (R:) avviene dalla sessione di lavoro individuale di ciascun utente da un PC in dominio aouts.it tramite l'icona "Computer" o "Risorse del Computer". I permessi di accesso alle cartelle di Struttura ("Reparto") vengono settati automaticamente sulla base dell'appartenenza gerarchica di un operatore alla struttura e viene perciò inserito "d'ufficio" nel relativo gruppo di dominio che consente l'accesso alla cartella e la mappatura del disco (R:).
È importante sottolineare che, a prescindere dal PC in dominio aouts.it dal quale l'utente lavora, il disco (R:) visualizzato è sempre lo stesso: quello della propria struttura a cui accede sempre con i diritti di accesso definiti per lui dal DIR-TD di struttura. La quantità massima di dati che ogni struttura potrà salvare è limitata. Questo perché l'unità di rete disco (R:) sul fileserver viene intesa come una zona di interscambio pregiata delle informazioni, dove gli utenti archiviano i documenti che risultano necessari per il normale svolgimento delle attività della struttura, e non come un archivio storico.
Nell'ambito della responsabilità del DIR-TD e delle visibilità che lo stesso ha autorizzato, è lecito salvare anche dati sensibili sul fileserver, fermo restando i principi di cui all'art. 6. In tal senso è possibile richiedere permessi di accesso puntuali a gruppi ristretti di utenti per specifiche sotto-cartelle, in maniera limitata e al solo scopo di effettuare trattamenti non eccedenti.

[5] Alla data di approvazione del presente documento (dicembre 2021)

Le necessità di condivisione/scambio e di archiviazione di dati e file che nascono in seno ad una struttura ma sono trasversali a più strutture (es. due o più SC) o a sotto-strutture (scambio all'interno del Dipartimento o del Distretto) vengono soddisfatte con le cartelle di tipo "Misto". I permessi vengono settati sulla base di puntuali richieste dei DIR-TD responsabili della cartella, tramite appositi gruppi di dominio (raggruppamenti logici di utenti) in cui gli operatori vengono inseriti. L'unita di rete mappata dagli operatori abilitati ad una cartella di tipo "Misto" è solitamente il disco (M:), il cui accesso avviene dalla sessione di lavoro individuale di ciascun utente da un PC in dominio aouts.it tramite l'icona "Computer" o "Risorse del Computer". Nel caso in cui un utente sia abilitato a più di una cartella di tipo "Misto", verrà mappata solo la prima in ordine alfabetico; le altre potranno essere raggiunte tramite il disco (V:), mappato da tutti gli utenti. Partendo quindi dal presupposto che le necessità di scambio trasversali a più strutture sono riconducibili sempre alla responsabilità di una unica struttura individuata quale "proponente/capofila", le cartelle hanno anche qui – come nel caso del disco (R:) – una configurazione per strutture aziendali (Struttura Complessa, Struttura Semplice Dipartimentale, Distretto, Dipartimento, Direzione) ma sono contraddistinte dal suffisso "_MISTO". In questo caso quindi la responsabilità degli accessi e dei dati archiviati è demandata al DIR-TD della struttura proponente/capofila.

Riassumendo, è possibile in linea teorica inserire un utente di dominio anche in più di una cartella di tipo "Reparto": questa fattispecie è fortemente sconsigliata perché l'utente mapperà con il disco (R:) solo la prima cartella in ordine alfabetico, analogamente all'abilitazione a più di una cartella di tipo "Misto". In questi casi l'utente, per raggiungere le altre cartelle a cui è abilitato, deve navigare all'interno dell'albero del fileserver utilizzando il disco (V:), ovvero in alternativa utilizzando il percorso di rete assoluto del fileserver stesso che potrà essere salvato sul desktop del singolo PC come collegamento.

8.2. Dominio ass1ad.fvgad.adds

Il dominio ass1ad.fvgad.adds è in dismissione.
Gli utenti che utilizzano ancora il dominio ass1ad.fvgad.adds possono accedere ad un fileserver che è stato consolidato in cloud SPC. All'interno del fileserver sono presenti diverse cartelle condivise (share). L'abilitazione alla singola share di rete viene eseguita puntualmente sulla base della specifica richiesta del DIR-TD. Con la migrazione al dominio unico aouts.it verranno spostati i dati/file applicando le politiche dettagliate nel paragrafo precedente.

8.3. Dominio ex AAS2 (ass2.sanita.fvg.it e aas2ad.fvgad.adds)

Gli utenti che utilizzano il dominio ex AAS2 possono accedere ad un fileserver per l'archiviazione sicura di file e cartelle. La continuità di servizio è garantita dall'alta affidabilità intrinseca del sistema, progettato per garantire nel tempo l'accesso ai dati, con ampi margini sulle fisiologiche rotture dei componenti hardware che lo costituiscono. Tutti i dati archiviati su questo fileserver sono soggetti a specifiche procedure di salvataggio (backup), gestite direttamente da Insiel che consentono di recuperare i file cancellati o modificati accidentalmente.

L'unita di rete disco (R:) – detto Reparto – è lo spazio disco del fileserver messo a disposizione di ciascuna struttura per la condivisione dei file e delle cartelle tra più o tutti gli operatori della struttura stessa.
L'accesso all'unita di rete disco (R:) avviene dalla sessione di lavoro individuale di ciascun utente da un PC in dominio aziendale.
È importante sottolineare che, a prescindere dal PC dal quale l'utente lavora, il disco (R:) visualizzato è sempre lo stesso: quello della propria struttura a cui accede sempre con i diritti di accesso definiti per lui dal DIR-TD di struttura. La quantità massima di dati che ogni struttura potrà salvare è limitata. Questo perché l'unità di rete disco (R:) sul fileserver viene intesa come una zona di interscambio

pregiata delle informazioni, dove gli utenti archiviano i documenti che risultano necessari per il normale svolgimento delle attività della struttura, e non come un archivio storico.
Nell'ambito della responsabilità del DIR-TD e delle visibilità che lo stesso ha autorizzato, è lecito salvare anche dati sensibili sul fileserver, fermo restando i principi di cui all'art. 6.

L'unita di rete disco (P:) – detto Utente – è lo spazio disco del fileserver messo a disposizione di ciascun utente/dipendente. Analogamente all'unita di rete disco (R:), l'accesso avviene dalla sessione di lavoro individuale di ciascun utente da un PC in dominio aziendale. I permessi di accesso alle condivisioni utente sono limitati unicamente all'utente stesso ed agli amministratori del dominio aziendale. Anche in questo caso, a prescindere dal PC dal quale l'utente lavora, l'unita di rete disco (P:) visualizzata è sempre la stessa: quella personale.

ART. 9 UTILIZZO DELLE RISORSE: SOFTWARE

L'utilizzo di qualunque software deve essere improntato alla consapevolezza e adeguato alla destinazione d'uso definita dal fabbricante e per gli scopi per cui il software stesso è stato reso disponibile da ASUGI.
È consentito esclusivamente l'uso dei software distribuiti ufficialmente da ASUGI (resi disponibili da ASUGI stessa o in ambito SISSR).
Ogni software utilizzato sui PC aziendali deve appartenere alla "whitelist" aziendale, prevista da normativa, dei software autorizzati. È vietato modificare la configurazione dei software.
Non è consentito scaricare software da internet né utilizzare software – anche se "portable" – se non previamente verificato ed inserito da SCIT nella whitelist aziendale. È vietata l'installazione di software non autorizzato in quanto possibile fonte di introduzione di malware e/o di alterazione della stabilità delle applicazioni presenti nell'elaboratore e potenziale pericolo per l'intera infrastruttura IT aziendale e regionale.
In generale ogni software introduce un rischio sul PC sul quale viene eseguito e sulle risorse dallo stesso accessibili e va gestito nel corso del suo intero ciclo di vita, perciò è buona prassi minimizzare il numero di software iscritti nella whitelist aziendale. Di conseguenza il Dir-TD deve comunicare a SCIT tramite i canali di assistenza ordinaria che un software non è più necessario in modo da consentire la disinstallazione e la rimozione dalla whitelist.

ART. 10 UTILIZZO DELLE RISORSE: HARDWARE

Non è consentito manomettere fisicamente qualunque dispositivo né modificare le impostazioni e le configurazioni con cui viene consegnato. Di conseguenza non sono consentiti, per esempio, l'installazione autonoma di periferiche e l'utilizzo di dispositivi di memorizzazione, comunicazione o altro (es. dischi esterni, pendrive, webcam, smatphone ecc.), anche ove tecnicamente possibile.
La SCIT si riserva la facoltà di disabilitare in qualsiasi momento le interfacce USB in quanto mezzi di possibile introduzione di malware ed esfiltrazione di dati.

Di norma ogni PC aziendale in dominio deve essere utilizzato collegato alla rete dati aziendale. È vietata la disconnessione di un PC fisso dalla rete dati. In generale i PC non devono essere lasciati inutilizzati e non devono mai risultare spenti per più di un mese (es. periodo di ferie) in modo da consentire gli aggiornamenti di sistema che prevedono periodici riavvi; per tale motivo anche nell'uso quotidiano è buona prassi spegnere il pc quotidianamente.
Tutti i PC portatili in dominio sono funzionanti solo per l'utilizzo – anche da remoto – su rete aziendale. In via transitoria, ove non ancora configurati in tal senso, devono essere collegati periodicamente (con frequenza almeno settimanale) alla rete dati aziendale per consentire gli aggiornamenti di sistema (es. antivirus e sistema operativo). La connessione a reti diverse, quali per

es, tramite cellulari e hotspot, è permessa solo al fine di instaurare la VPN verso la rete aziendale. Sono vietate connessioni internet dirette.
Va prestata la massima attenzione nell'uso di dispositivi mobili non in dominio, limitando il più possibile la connessione a reti esterne e la navigazione internet e l'installazione di applicazioni. Se utilizzati per la posta aziendale deve essere sempre impostata la schermata di blocco.

È vietato l'utilizzo di apparati di rete non installati da SCIT (es. switch utilizzati per collegare più dispositivi ad un unico punto rete).
Analogamente è vietato collegare alla rete aziendale (non guest) dispositivi privati oltre a qualunque dispositivo non previamente autorizzato da SCIT, anche ove tecnicamente possibile.

ART. 11 UTILIZZO DI INTERNET E DEI SOCIAL NETWORK

La navigazione in internet permessa da PC aziendali è filtrata da sistemi automatici che impediscono l'accesso a siti classificati come potenzialmente pericolosi nonché l'utilizzo di specifiche funzionalità. Questo abbassa il rischio ma non lo annulla.
È quindi comunque essenziale e doveroso il comportamento virtuoso ed attento degli utilizzatori. L'utente è tenuto, nel corso della navigazione, a leggere con attenzione qualsiasi finestra, pop up o avvertenza prima di proseguire nella navigazione stessa. Tra l'altro è sempre opportuno verificare l'affidabilità del titolare del sito ovvero navigare solo su siti tradizionali e ben conosciuti.
La confidenzialità della comunicazione generica attraverso il web è estremamente limitata in quanto i messaggi, transitando nella rete pubblica, possono essere facilmente visionati da terzi non autorizzati.
Molti siti utilizzano canali crittografati e questo è evidenziato nel browser con un piccolo lucchetto chiuso. Quindi, qualora una comunicazione di dati sensibili o di informazioni riservate via web sia lecita, è comunque sempre necessario accertarsi che vi sia la protezione della comunicazione attraverso il sistema crittografico SSL (Secure Socket Layer, https:\\).
La SCIT ha facoltà di porre limiti alla navigazione internet escludendo dalla navigazione siti non attinenti agli scopi aziendali o sospendendo i permessi d'accesso assegnati.

È vietato postare qualunque foto e video che ritragga ambienti aziendali su blog e social network o di renderli in qualsiasi modo accessibili via internet, anche se risalenti ad epoca precedente alla data di rilascio del presente regolamento. Eventuali necessità dovranno essere vagliate dal Servizio di "Comunicazione, Relazioni Esterne Aziendali e Ufficio Stampa".
Per quanto riguarda i sistemi di messaggistica istantanea (per es. WhatsApp), questi non sono strumenti aziendali di lavoro. In generale non vanno utilizzati.

ART. 12 UTILIZZO DELLA POSTA ELETTRONICA

I moderni mezzi di comunicazione sono risorse che offrono opportunità anche per l'azione aziendale, ma vengono ampliamente sfruttati dai malintenzionati per azioni di phishing e di propagazione di malware, è quindi indispensabile che le attività degli utilizzatori siano sempre improntate al buon senso ed alla prudenza, che rimangono il presupposto per un corretto e sicuro impiego di tali mezzi di comunicazione.
In generale non vanno mai aperti allegati o link se non provenienti da fonti sicure. Considerato che è facile modificare la provenienza evidenziata facendo sembrare una mail maligna proveniente da fonte sicura, è sempre opportuno non aprire allegati o link che non ci aspettiamo da quella fonte o che non sono coerenti con quanto quella fonte sicura ci invia regolarmente.
Le nuove campagne di phishing utilizzano messaggi dall'aspetto legittimo e con allegati o collegamenti maligni incorporati nel testo, ed utilizzano account e-mail "violati" per inviare malware in risposta ad una comunicazione già intercorsa. L'e-mail maligna diventa parte quindi di una conversazione

legittima e continuativa, e può essere intercettata solo se l'attenzione dell'utente è particolarmente alta.

12.1. Posta Elettronica Ordinaria (PEO, cosiddetta e-mail)

Ogni assegnatario di casella di posta elettronica aziendale è responsabile del corretto utilizzo della stessa. Va prestata particolare attenzione nella selezione dei destinatari dei messaggi verificando la correttezza degli indirizzi dei destinatari prima dell'invio, con particolare attenzione ad omonimi aziendali o comunque ricompresi nella rubrica globale (es. dipendenti regionali). Il campo Oggetto va compilato sempre con indicazione dell'argomento; chi risponde manterrà sempre lo stesso Oggetto al fine di conservare una struttura storica ordinata dei messaggi inviati e ricevuti, "agganciandoli" nella conversazione. È opportuno non inviare una e-mail ad un numero elevato di destinatari. Qualora indispensabile va valutata l'opportunità di utilizzare il campo "Ccn:" anziché il campo "A:" o "Cc:" affinché i destinatari non si vedano tra di loro.
Può essere richiesta la ricevuta di corretto ricevimento con la consapevolezza che le varie conferme non garantiscono una vera lettura e comprensione del messaggio da parte del destinatario. È comunque buona norma non richiedere indiscriminatamente la ricevuta di ritorno da parte del destinatario.
Gli allegati devono avere dimensione massima di 20 MB (possibilmente senza funzioni macro).
Gli utenti sono invitati a leggere quotidianamente la posta elettronica aziendale e a rispondere in tempi ragionevoli alle e-mail ricevute; è buona prassi rispondere a tutti e mantenere la catena di mail. Solo nel caso di mail *circolari* ossia inviate a molti destinatari in modo generico per la risposta è spesso opportuno usare la funzione "Rispondi" anziché "Rispondi a tutti".

Le e-mail vanno tenute ordinate ed organizzate e vanno eliminate quando non più necessarie, infatti l'applicativo aziendale di posta elettronica non è un applicativo di gestione documentale ma un sistema di scambio estemporaneo di informazioni.
Una quantità elevata di e-mail nella casella di posta determina l'impossibilità di invio e ricezione; si suggerisce quindi di prestare attenzione agli avvisi di casella troppo piena.
È vietato l'invio di messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità presunte. È vietata la generazione di spam.
I messaggi di SPAM ricevuti vanno segnalati tempestivamente alla casella regionale antivirus-alert (av-alert@insiel.it).

12.2. Posta Elettronica Certificata (PEC)

ASUGI ha un indirizzo di PEC, sia in invio che in ricezione, collegato al protocollo generale aziendale. L'indirizzo è asugi@certsanita.fvg.it. Le regole di utilizzo sono pubblicate sul sito internet.
Considerato che il servizio di posta elettronica certificata fornisce garanzie di certezza dell'identità del mittente, data e ora di trasmissione e di ricezione opponibili ai terzi, di integrità e non modificabilità degli allegati trasmessi unitamente al messaggio di posta elettronica, nonché di riservatezza, è possibile in taluni casi utilizzare la PEC per l'invio di dati sensibili.

ART. 13 ATTIVITÀ LAVORATIVA A DISTANZA

Nel caso di prestazione dell'attività lavorativa a distanza con l'utilizzo di PC privati, finché autorizzata, la connettività alla postazione di lavoro aziendale sarà garantita esclusivamente per mezzo dei sistemi VPN ASUGI. La connessione VPN di tipo client-to-site è effettuata per mezzo di credenziali personali. A valle dell'instaurazione della connessione VPN, il collegamento alla postazione di lavoro aziendale dovrà avvenire con lo strumento integrato di Microsoft Windows denominato Remote Desktop Protocol (RDP). Si rimanda all'accordo individuale ed eventualmente anche alle specifiche istruzioni date agli utenti al momento dell'abilitazioni. In generale comunque il PC deve essere dotato di sistema operativo correttamente licenziato e non obsoleto ossia dichiarato in supporto del fabbricante e

costantemente e tempestivamente aggiornato dal punto di vista della sicurezza; dotato di sistema antivirus attivo, anche esso costantemente e tempestivamente aggiornato. Sul PC utilizzato possono essere installati solamente software regolarmente licenziati e in supporto tecnico del produttore, e periferiche sicure. La connessione ad Internet per l'instaurazione della VPN può essere effettuata da reti personali anche Wi-Fi, purché con protocollo almeno WPA2-PSK e adeguatamente protette da password robusta. La password di dominio utilizzata per l'accesso alla VPN ed al PC remoto (ufficio) non dovranno mai essere memorizzate sul PC locale.

Nel caso di prestazione dell'attività lavorativa a distanza con l'utilizzo di PC aziendali, questi dovranno essere in modalità "Always-On".

Tutto quanto indicato nel seguente regolamento si intende applicabile anche durante l'attività lavorativa a distanza.

ART. 14 ASSISTENZA TECNICA

Le modalità di richiesta di intervento tecnico per malfunzionamenti delle risorse informatiche e telematiche sono pubblicate nella pagina intranet.
Tutti gli utenti sono invitati a eseguire semplici operazioni di verifica del funzionamento delle risorse informatiche e telematiche in uso (corretta connessione delle prese e dei cavi di collegamento, alimentazione elettrica, ecc.) prima di attivare l'assistenza tecnica.
È cura di ogni utente segnalare tempestivamente qualunque anomalia di funzionamento venga rilevata durante l'utilizzo delle risorse informatiche e telematiche.
Il servizio di assistenza tecnica non chiederà mai per nessun motivo di comunicare via e-mail, telefono, fax o altro mezzo le proprie password personali o altre informazioni riservate. È vietato comunicare queste informazioni a chiunque.
L'attività di assistenza ed altre operazioni di manutenzione ed aggiornamento del software vengono espletate – ove del caso – da personale afferente a SCIT, dipendente o di fornitore esterno, anche con strumenti di controllo remoto che consentano di compiere le operazioni necessarie attraverso la rete locale anziché recarsi sul posto. Questa modalità operativa agevola notevolmente l'efficacia degli interventi di assistenza tecnica. L'intervento in teleassistenza viene generalmente effettuato su richiesta dell'utente. Nell'ambito di attività di manutenzione preventiva programmata o azioni proattive o a seguito di guasti e malfunzionamenti rilevati in autonomia, personale tecnico della SCIT potrà intervenire da remoto eventualmente anche accendendo il PC.

ART. 15 MONITORAGGIO DELL'USO DELLE RISORSE

Per garantire la sicurezza dell'infrastruttura IT, delle applicazioni e dei dati, l'azienda effettua sia monitoraggi continui e sistematici sul buon funzionamento dei sistemi che monitoraggi a campione (non sistematici) sull'uso delle risorse informatiche e telematiche da parte degli utenti.
In particolare il Direttore SCIT tramite persona da lui individuata, nell'ambito dell'espletamento delle funzioni aziendali:
-Ha la facoltà di accedere in qualunque momento a qualsiasi dispositivo; tra l'altro può in qualunque momento procedere alla rimozione di qualsiasi file o applicazione che riterrà essere pericolosa per la sicurezza IT di ASUGI, o semplicemente inadeguata, sia sui PC che sulle unità di rete.
-Effettua dei monitoraggi sui dati di navigazione Internet - tracciati dai firewall aziendali - con la finalità di garantire il corretto ed efficiente funzionamento dei servizi nonché per verificare che i comportamenti non siano illeciti o lesivi per l'azienda. Potrà quindi essere esaminato il traffico internet per tipologia di destinazione e per quantità di traffico, con dettagli su data, ora, durata della connessione e quantità di traffico, a partire dal traffico generato dall'entrata in vigore del presente

regolamento, anche con analisi dei report standard messi a disposizione dai firewall di ultima generazione. Si evidenzia che la navigazione in incognito è sempre comunque riferibile al dipendente loggato al PC, quindi i monitoraggi di cui sopra comprendono anche la navigazione eseguita con modalità "in incognito" con qualunque browser.
-Effettua anche senza richiesta dell'utente interventi in teleassistenza qualora siano riscontrati malfunzionamenti o la violazione delle misure di sicurezza aziendali. A tal fine potrà avvalersi di strumenti di controllo remoto che consentano di compiere le operazioni necessarie attraverso la rete locale anziché recarsi sul posto. Detti interventi, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire l'operatività dell'Azienda, si applica anche in caso di assenza prolungata o di impedimento dell'utente, qualora non sia possibile procedere altrimenti.

Queste attività sono affidate agli "Amministratori di sistema" afferenti a SCIT abilitati alle diverse funzioni. I soggetti che operano quali amministratori o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi sono edotti e consapevoli delle linee di condotta da tenere, attraverso un'adeguata attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto delle comunicazioni. Essi svolgeranno solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

ART. 16 NORME FINALI E TRANSITORIE

Il presente regolamento ha effetto dalla data di pubblicazione del decreto di approvazione e contestualmente vengono disapplicati i precedenti regolamenti in materia.

ART. 17 ARCHIVIAZIONE

Il presente regolamento viene archiviato e mantenuto per tre anni.
L'accesso alla documentazione viene garantito dalla Rete internet/Intranet aziendale

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: ANDREA LONGANESI
CODICE FISCALE: LNGNDR61R19A547T
DATA FIRMA: 24/12/2021 14:28:07
IMPRONTA: 0A240EBDD41248352441541849C00B514DD36D3942C433E2DA08F2FCF2BBC389
4DD36D3942C433E2DA08F2FCF2BBC3898921545357F7F36A4BED98588AD27A0F
8921545357F7F36A4BED98588AD27A0F4EF38DFE4B06E4C9C96D9CC1A8D65E4D
4EF38DFE4B06E4C9C96D9CC1A8D65E4D545B6EF68166912D9CE0860973AA7943

NOME: EUGENIO POSSAMAI
CODICE FISCALE: PSSGNE59M27C957L
DATA FIRMA: 24/12/2021 15:03:24
IMPRONTA: 5A717B4B8DDFE5886B515B3B9AF3D7215DDD9F662E6BFC26D15A904D42D2FF72
5DDD9F662E6BFC26D15A904D42D2FF72B445FEA152C798398E81CD12F50B4C11
B445FEA152C798398E81CD12F50B4C11B74E2C069B1B006399C1FF8B6D4E3C5F
B74E2C069B1B006399C1FF8B6D4E3C5FC54EA3B2E2FBC0215EC7599495166A60

NOME: ANTONIO POGGIANA
CODICE FISCALE: PGGNTN64M30C743F
DATA FIRMA: 24/12/2021 15:36:22
IMPRONTA: 6C7AD962D51EA7619BE83FA62FCA62B88DBF529270A0B895377CB3EA2D4DC919
8DBF529270A0B895377CB3EA2D4DC9199783DFD20BA13E6CA34E725765E6EC4F
9783DFD20BA13E6CA34E725765E6EC4F5CEC533445D6187691CC94304948A3C7
5CEC533445D6187691CC94304948A3C772ECD6CCFC5A00D8CBCCA9E4B00B3670

NOME: FABIO SAMANI
CODICE FISCALE: SMNFBA57C03L424I
DATA FIRMA: 24/12/2021 16:55:44
IMPRONTA: 4AAD9090C7F43A95518753F18E971A82FFDD3AEB50692EDFDF9FC0AF250EC982
FFDD3AEB50692EDFDF9FC0AF250EC982C2AA82B103CF7B56D1DBF2E6F0540DEC
C2AA82B103CF7B56D1DBF2E6F0540DECF1D59BE56C18CE7594B7B2270C52595D
F1D59BE56C18CE7594B7B2270C52595DA00572702A54E9FEC223FC2B2901D166