ASU FC
Azienda sanitaria universitaria Friuli Centrale

DECRETO
DEL DIRETTORE GENERALE

dott. Denis Caporale

nominato con deliberazione della Giunta Regionale
n. 591 del 21 aprile 2021

N. 481 **DEL 29/04/2022**

AVENTE AD OGGETTO:

Adozione Regolamento aziendale disciplinante l'utilizzo delle risorse informatiche, internet e posta elettronica ordinaria dell'Azienda sanitaria universitaria Friuli Centrale.

Con la partecipazione per l'espressione dei pareri di competenza:

del Direttore Amministrativo avv. Francesco Magris
del Direttore Sanitario dott.ssa Laura Regattin
del Direttore dei Servizi Sociosanitari Facente Funzioni dott. David Turello

OGGETTO: Adozione Regolamento aziendale disciplinante l'utilizzo delle risorse informatiche, internet e posta elettronica ordinaria dell'Azienda sanitaria universitaria Friuli Centrale.

PREMESSO che

- il (Piano Triennale per l'informatica nella Pubblica Amministrazione 2017-2019, 2019-2021, 2020-2022), ha fissato obiettivi, priorità e regole per diffondere e rendere omogeneo l'utilizzo delle tecnologie ICT, quali leva strategica per la reingegnerizzazione e l'ottimizzazione dei processi della PA e per l'erogazione di servizi a cittadini e imprese;
- la diffusione delle tecnologie informatiche e telematiche ed il progressivo passaggio della società verso modelli di comunicazione sempre più integrati ed interconnessi rendono fondamentale, per ogni realtà organizzativa e lavorativa, lo sviluppo di una cultura della sicurezza del proprio patrimonio informativo e della tutela dei diritti degli interessati;
- l'Azienda Sanitaria Universitaria Friuli Centrale – ASU FC – nell'ottica di uno svolgimento proficuo e più agevole della propria attività, mette a disposizione dei propri dipendenti e collaboratori apparecchiature informatiche e mezzi di comunicazione;
- l'Azienda Sanitaria Universitaria Friuli Centrale – ASU FC – è il soggetto che determina le finalità ed i mezzi del trattamento dei dati personali ed è competente in merito al rispetto dei principi finalizzati alla tutela e protezione dei dati stessi.

RICHIAMATI

- il Regolamento Generale sulla Protezione dei Dati (GDPR, *General Data Protection Regulation* - Regolamento UE 2016/679) pubblicato in Gazzetta Ufficiale Europea il 04/05/2016, entrato in vigore dal 24/5/2016, e applicabile a partire dal 25/05/2018;
- il Decreto Legislativo n.196 del 30/06/2003 c.d. "Codice in materia di protezione dei dati" (di seguito "Codice Privacy") e s.m.i.;
- il "Piano Triennale per l'Informatica nella Pubblica Amministrazione", approvato dall'Agenzia per l'Italia Digitale (AgID), nelle versioni 2017-2019, in data 13/05/2017, e 2019-2021, in data 11/03/2019;
- Provvedimento del Garante per la protezione dei dati personali n. 13 del 01/03/2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" (di seguito "Provvedimento");
- Decreto legislativo n. 82 del 7/03/2005 c.d. "Codice dell'Amministrazione Digitale" e s.m.i. (di seguito "CAD");

- Legge n.633 del 22/04/1941 c.d. "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio";
- Legge n. 300 del 20/05/1970 c.d. "Statuto dei lavoratori";
- Circolare Agenzia per l'Italia Digitale n° 2 del 18/04/2017 recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni (DPCM del 1° agosto 2015)" (di seguito "Circolare AgID").

PRESO ATTO che l'ASU FC, nel rispetto di quanto stabilito dal Piano triennale per l'informatica nella Pubblica Amministrazione 2020-2022 nell'ambito della sicurezza cibernetica, deve:

- garantire la disponibilità, l'integrità e la riservatezza del patrimonio informativo dell'Ente nonché il rispetto dei principi di *privacy* previsti dalle normative vigenti;
- monitorare e tenere sotto controllo l'evoluzione continua delle minacce cibernetiche che mettono a rischio sistematico la disponibilità, l'integrità e la riservatezza del sistema informativo dell'Ente con la conseguente possibilità di causare interruzione dei servizi telematici a cittadini ed imprese;
- seguire un approccio omogeneo per affrontare la sicurezza, con l'obiettivo di ridurre il rischio legato alla minaccia cyber, anche attraverso il monitoraggio periodico dell'infrastruttura tecnologica mediante l'uso di strumenti di analisi delle vulnerabilità (VA - *Vulnerability Assessment*) e degli eventi (SIEM - *Security Information and Event Management*);
- mantenere in efficienza, ottimizzare l'uso e prevenire utilizzi indebiti delle Dotazioni;
- evitare che gli utenti possano esporre sé stessi e/o l'ASUFC a sanzioni pecuniarie o penali, derivanti da un uso scorretto o illecito delle Dotazioni, nonché esporre l'ASU FC a conseguenze pregiudizievoli, in relazione al suo patrimonio e/o alla sua immagine;
- recepire e dare attuazione alle disposizioni normative e ai principi previsti dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito anche solo "GDPR"), nonché dei Provvedimenti emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante").

CONSIDERATO che

- la minaccia cibernetica cresce continuamente in quantità e qualità, determinata anche dall'evoluzione delle tecniche di ingegneria sociale

volte a ingannare gli utenti finali dei servizi digitali sia interni alla PA che fruitori dall'esterno;

- risulta fondamentale adottare tutte le iniziative tese a salvaguardare l'integrità, la disponibilità, la continuità nella fruibilità dei dati, anche attraverso l'adozione di misure di sicurezza e di soluzioni atte a garantire la continuità di funzionamento dei sistemi informativi.

CONSIDERATA la necessità di disciplinare unitariamente in tutte le articolazioni organizzative aziendali la materia dell'utilizzo delle risorse informatiche, internet e posta elettronica ordinaria al fine di ottemperare alle esigenze di continuità dei servizi costituenti la *mission* aziendale;

DATO ATTO che non rientra tra gli scopi del Regolamento il controllo a distanza e/o in forma occulta delle opinioni, abitudini e/o dell'attività dei suoi dipendenti, che rimangono strettamente vietati e non consentiti e che pertanto, nel rispetto delle previsioni di cui agli artt. 4 e 8 della Legge 20 maggio 1970, n. 300 (di seguito anche solo "Statuto dei Lavoratori"), ASU FC intende anche disciplinare, con il Regolamento, le modalità di raccolta ed utilizzo delle informazioni e dei dati trattati tramite le Dotazioni, informando circa l'esercizio dell'eventuale potere disciplinare del ASU FC nei confronti dei dipendenti, qualora si verificasse ed accertasse - secondo le procedure e nel rispetto delle garanzie e tutele oggetto delle previsioni che seguono - un uso improprio e/o non autorizzato delle Dotazioni;

RITENUTO di disciplinare l'utilizzo delle risorse informatiche, internet e posta elettronica ordinaria secondo le disposizioni di cui al regolamento allegato che forma parte integrante del presente provvedimento;

RICHIAMATO il Modello Organizzativo Privacy (MOP) dell'Azienda Sanitaria Universitaria Friuli Centrale;

CONSIDERATO il parere positivo del D.P.O. e del Responsabile *privacy* dell'Azienda Sanitaria Universitaria Friuli Centrale;

DATO ATTO che il presente provvedimento è conforme alla proposta del responsabile del procedimento;

DATO ATTO che la proposta di Regolamento Aziendale sull'Utilizzo delle Risorse Informatiche, Internet e Posta Elettronica sarà oggetto di informativa alle Organizzazioni Sindacali relativamente all'impatto sui diritti dei lavoratori;

PRESO ATTO che il Direttore della Struttura Tecnologie Informatiche nel proporre il presente atto attesta la regolarità tecnica ed amministrativa, la

legittimità e congruenza dell'atto con le finalità istituzionali dell'Ente, l'assenza di conflitto di interessi, stante anche l'istruttoria effettuata a cura del Responsabile del Procedimento;

ACQUISITO il parere favorevole del Direttore sanitario, del Direttore amministrativo e Del direttore dei servizi sociosanitari f.f., per quanto di rispettiva competenza;

DECRETA

per i motivi di cui in premessa, che qui si intendono integralmente riportati, di:

1) approvare il "Regolamento Aziendale sull'Utilizzo delle Risorse Informatiche, Internet e Posta Elettronica" di cui all'allegato 1, parte integrante del presente provvedimento;

2) dare mandato al responsabile del procedimento di adempiere a tutte le incombenze successive all'emanazione del presente provvedimento, tra cui provvedere alla comunicazione della "politica per il corretto utilizzo degli strumenti informatici" agli utenti tutti, nelle forme che riterrà più efficaci;

3) dare atto che il presente provvedimento è immediatamente esecutivo sulla base di quanto previsto dall'art. 4 comma 2 LR 21/1992 e ss.mm.ii.

Letto, approvato e sottoscritto digitalmente

Il Direttore Amministrativo
avv. Francesco Magris

Il Direttore Sanitario
dott.ssa Laura Regattin

Il Direttore dei Servizi Sociosanitari Facente Funzioni
dott. David Turello

Il Direttore Generale
dott. Denis Caporale

Allegati:

1	TI_RG_01_Risorse informatiche - ver. 01.pdf

Uffici notificati:

Tecnologie Informatiche

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: FRANCESCO MAGRIS
CODICE FISCALE: MGRFNC69D27G888F
DATA FIRMA: 29/04/2022 15:14:06
IMPRONTA: 4044EC1F8CE5B5B6CE2673FC4B3354169A25FD0183DA2FA262DD21ACA7324554
9A25FD0183DA2FA262DD21ACA7324554E3A23EB9146B840A56CDA4BAA1E9DA1A
E3A23EB9146B840A56CDA4BAA1E9DA1A256758B3011350E4D266D035815E0A7F
256758B3011350E4D266D035815E0A7F637E58B0297E28E6FEB3F3F3834C5C76

NOME: DAVID TURELLO
CODICE FISCALE: TRLDVD77S13G284T
DATA FIRMA: 29/04/2022 15:29:38
IMPRONTA: 20CB3E4D1C5C874C4E5D1FF5652B8C3B8541761F8E5E4CBD6D3C307968F7C95F
8541761F8E5E4CBD6D3C307968F7C95F09FCCB90528D597E3A134638320CEA35
09FCCB90528D597E3A134638320CEA35B4317D54DC396F5FB3477D5284180EEB
B4317D54DC396F5FB3477D5284180EEB1E9230B7E59CC02E3C898948FE907122

NOME: DENIS CAPORALE
CODICE FISCALE: CPRDNS75M11C758X
DATA FIRMA: 29/04/2022 15:48:04
IMPRONTA: 4BABD23CDB6B772FBE0D89FC6D4072BE472FC8A76F0057D4ACF6B54EF11F5AF3
472FC8A76F0057D4ACF6B54EF11F5AF3C29DC307DB564264FDC614541AECC4AB
C29DC307DB564264FDC614541AECC4AB7444A15CCD6E582199AE9830D8F294F8
7444A15CCD6E582199AE9830D8F294F8EB14166F63B61BA5F67FA7BCFBA6B214

NOME: LAURA REGATTIN
CODICE FISCALE: RGTLRA70L69L483A
DATA FIRMA: 29/04/2022 17:24:35
IMPRONTA: 2CD8FF496BE0AF176E7BAFFD2A98E849A78740833F3E51284792C6018FB650DD
A78740833F3E51284792C6018FB650DDB2AD04C9537264C48B6E3150517F7535
B2AD04C9537264C48B6E3150517F7535213044629FD40FD5034DD93E521DD889
213044629FD40FD5034DD93E521DD889C884C536D63BB79D845999A679D79024

REGOLAMENTO AZIENDALE SULL'UTILIZZO DELLE RISORSE INFORMATICHE, INTERNET E POSTA ELETTRONICA ORDINARIA

Redazione	Verifica	Approvazione
Referente per la redazione del documento: ing. Tiziano Tommasini	SC Tecnologie Informatiche dott. Piero Pascolo Ufficio Privacy Avv. Stefano Bergagna Responsabile Protezione Dati Avv. Fabio Romano Balducci	Decreto del Direttore Generale n._____ del __/__/____
Documento in ADWeb	Documento in ADWeb	Documento in ADWeb

Parola chiave 1	Parola chiave 2	Parola chiave 3
Informazioni e comunicazione	Risorse informatiche	Internet, posta elettronica

INDICE

1. Matrice delle versioni del documento

Codifica	Versione	Data	Motivo della modifica
TIC_RG_01	01	21/01/2022	Redazione documento unico per l'Azienda Sanitaria Universitaria Friuli Centrale.

2. Scopo e campo di applicazione

2.1. Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, l'accesso alla rete *Internet* dai *Personal Computer*, espone *l'Azienda Sanitaria Universitaria Friuli Centrale* (di seguito "Azienda") e gli utenti (dipendenti e Personale autorizzato) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla possibile violazione di specifiche disposizioni di legge (protezione dei dati, *privacy* e diritto d'autore, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa. In questo senso è fortemente sentita la necessità di attivare opportune misure di controllo sull'utilizzo delle tecnologie informatiche al fine di sensibilizzare gli utenti e prevenire eventuali usi scorretti delle stesse. Laddove in particolare non si possa intervenire mediante strumenti elettronici e/o automatismi di prevenzione e/o controllo, è comunque importante disporre di regolamenti che indirizzino i dipendenti al corretto utilizzo delle risorse messe loro a disposizione dall'Azienda.

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Azienda ha quindi adottato un regolamento interno al fine di disciplinare i comportamenti degli Utenti per prevenire l'accadimento di eventi avversi che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati. I controlli sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione – essendo le dotazioni oggetto del presente regolamento strumenti di lavoro la cui utilizzazione personale è preclusa – quanto il diritto del lavoratore a non vedere invasa la propria sfera personale ed il conseguente diritto alla riservatezza ed alla dignità, così come sanciti dallo Statuto dei Lavoratori e dalle norme vigenti.

Questo regolamento viene incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici e/o telematici da parte degli utenti, in particolare alla luce delle Linee Guida comprese nel Provvedimento citato di seguito emanato dal Garante per la protezione dei dati personali (di seguito "Garante") relativo a posta elettronica ed *Internet* – (Del. n. 13 del 1° marzo 2007) e della legislazione cogente in materia di responsabilità amministrativa delle persone giuridiche (D.lgs. n. 231 del 08 giugno 2001 e s.m.i.) e fornendo informazioni in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Allo scopo di rappresentare agli Utenti il quadro normativo di riferimento si specifica che le principali fonti normative in materia sono le seguenti:

- Regolamento Generale sulla Protezione dei Dati (UE) n. 2016/679 (di seguito "GDPR");

- Decreto Legislativo n.196 del 30/06/2003 c.d. "Codice in materia di protezione dei dati" (di seguito "Codice Privacy") e s.m.i.;
- Provvedimento del Garante per la protezione dei dati personali n. 13 del 01/03/2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" (di seguito "Provvedimento");
- Decreto legislativo n. 82 del 7/03/2005 c.d. "Codice dell'Amministrazione Digitale" e s.m.i. (di seguito "CAD");
- Legge n.633 del 22/04/1941 c.d. "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio";
- Legge n. 300 del 20/05/1970 c.d. "Statuto dei lavoratori";
- Circolare Agenzia per l'Italia Digitale n° 2 del 18/04/2017 recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni (DPCM del 1° agosto 2015)" (di seguito "Circolare AgID").

L'inosservanza delle norme sulla *privacy* può comportare sanzioni di natura civile e penale per l'incaricato e per l'Azienda per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

2.2. Finalità

L'Azienda, nell'ottica dello svolgimento della propria *mission* e raggiungimento degli obiettivi istituzionali mette a disposizione dei propri dipendenti e del personale autorizzato idonee apparecchiature informatiche, strumenti di produttività e mezzi di comunicazione (*Personal Computer*, *notebook, tablet*, accesso alla rete aziendale, accesso alle procedure aziendali, casella di posta elettronica, accesso alla rete *Internet*, ecc.). Il presente documento disciplina le modalità d'uso delle risorse informatiche aziendali, stabilendo gli obblighi dell'utenza e dell'Azienda, nell'ottica di una più stretta e leale collaborazione nel rispetto delle reciproche attribuzioni.

Le finalità del presente regolamento sono:

a) fornire indicazioni anche operative agli utenti con l'obiettivo di garantire e salvaguardare la sicurezza e protezione dei dati trattati in Azienda nel rispetto della normativa vigente;

b) regolamentare l'utilizzo delle risorse informatiche in modo che siano impiegate in maniera efficace, produttiva ed orientata al raggiungimento degli obiettivi aziendali;

c) garantire la sicurezza e la prevenzione del danneggiamento delle risorse informatiche, dei servizi e delle attività legate all'utilizzo di *Internet*, della posta elettronica ordinaria, ecc.;

d) garantire la tutela del dipendente e del personale autorizzato all'uso delle risorse informatiche.

Il patrimonio informativo dell'Azienda è costituito dall'insieme di dati ed informazioni necessari allo svolgimento della *mission* aziendale e/o istituzionale. Tale patrimonio deve essere tutelato mediante l'adozione di una serie di misure di natura tecnologica, organizzativa, procedurale e normativa, commisurate alla criticità ed al valore delle informazioni stesse, e derivate nel rispetto dei tre requisiti fondamentali della sicurezza delle informazioni, ovvero:

- la riservatezza, orientata ad assicurare che l'informazione sia disponibile solo agli utenti autorizzati;
- l'integrità, volta a salvaguardare la completezza, l'accuratezza e la conformità dell'informazione durante l'acquisizione, la conservazione, l'elaborazione e la presentazione;
- la disponibilità, finalizzata ad assicurare che gli utenti autorizzati abbiano accesso alle informazioni ed agli elementi architetturali associati, quando se ne evidenzi l'effettivo bisogno attraverso opportune richieste.

A maggior tutela dell'aspetto di sicurezza del patrimonio informativo aziendale, è inoltre utile prendere in considerazione ed assicurare il rispetto anche dei seguenti ulteriori requisiti:

- l'autenticità, in termini di garanzia della provenienza dell'informazione;
- il non ripudio, avente lo scopo di assicurare che l'informazione sia protetta da falsa negazione di ricezione, trasmissione, creazione, trasporto, consegna e ricevuta.

La mancanza di adeguati livelli di sicurezza connessi a tali requisiti può esporre i dati e le informazioni a rischi di sicurezza che possono avere impatti negativi sull'attività aziendale, quali ad esempio: danni di immagine, mancata soddisfazione da parte dell'utente/paziente, danni di natura economica e finanziaria, ecc.. La normativa prevede, inoltre, sanzioni legate alla violazione delle normative vigenti.

L'Azienda garantisce che i dati informatizzati da essa gestiti, nonché i sistemi di elaborazione dati e gli strumenti di telecomunicazioni, non saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114 e 171, Codice Privacy; artt. 4 e 8, L. 20 maggio 1970, n.300 – Statuto dei Lavoratori), se non nei limiti consentiti dallo Statuto dei Lavoratori, così come modificato dal D. Lgs. 151/2015 ("Jobs Act") e comunque previa informativa ai dipendenti interessati.

Sarà cura dell'Utente accertarsi se siano state pubblicate nuove versioni del presente regolamento e adottare comportamenti congrui a quanto prescritto relativamente ai propri ambiti specifici di competenza e di attività.

2.3.Ambiti di applicazione

Il documento è redatto in conformità ai principi delle normative vigenti.

I rapporti tra l'Azienda e gli Utenti si ispirano a principi di trasparenza e leale collaborazione.

Il documento si applica a:

- tutti gli Utenti che utilizzano le risorse informatiche di proprietà dell'Azienda;
- tutte le risorse informatiche di proprietà dell'Azienda e/o messe a disposizione nell'ambito del Sistema Informativo Integrato Regionale (in seguito "SIIR");
- tutte le operazioni di accesso a informazioni registrate ed archiviate elettronicamente tramite risorse informatiche aziendali;
- tutte le forme di comunicazione operate attraverso *Internet* e posta elettronica ordinaria.

3. Destinatari

Il documento è destinato a tutto il personale dipendente ed al personale autorizzato (di seguito "Utenti"), a prescindere dal rapporto contrattuale con l'Azienda (ivi compresi consulenti, convenzionati, aziende esterne legate da contratti di fornitura e/o servizi o altri individui in possesso di specifiche credenziali di autenticazione alle quali è consentito l'accesso alle risorse aziendali), senza distinzione di ruolo e/o livello, che si trovano ad operare con le risorse informatiche aziendali.

4. Contenuti

4.1. Utilizzo delle risorse informatiche aziendali

L'utilizzo delle risorse informatiche aziendali e di quelle messe a disposizione dal SIIR e delle banche dati, è riservato agli Utenti dell'Azienda e ad altri soggetti espressamente ed esplicitamente autorizzati dal Responsabile della Struttura di appartenenza, il quale dovrà tempestivamente comunicare qualsiasi modifica relativa all'organico che richieda l'attivazione, la sospensione e/o la revoca dell'autorizzazione all'accesso alle risorse informatiche e banche dati.

In caso di trasferimento in altra Struttura tutte le apparecchiature tecnologiche assegnate ad un Utente restano in uso presso la Struttura originaria, salvo esplicita autorizzazione della Direzione Strategica allo spostamento o riassegnazione delle stesse.

È compito della Struttura del Sistema Informativo Aziendale valutare lo stato di obsolescenza del materiale affidato e prevedere dei piani di sostituzione dello stesso compatibilmente con le risorse economiche a disposizione.

Le risorse informatiche aziendali sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente professionali e lavorativi compresi quelli di ricerca e didattica. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di gestione/manutenzione e, soprattutto, introdurre potenziali vulnerabilità al sistema di sicurezza aziendale con conseguente aumento del rischio. Ciò vale sia per le risorse condivise (risorse di rete, stampanti di rete, ecc.), sia per quelle affidate al singolo Utente (*Personal Computer*, portatili, programmi e/o applicazioni, periferiche, stampanti locali, ecc.).

Le risorse informatiche affidate al singolo Utente sono strumenti di lavoro appartenenti al patrimonio aziendale e pertanto devono essere custoditi in modo appropriato. Il verificarsi di alcune situazioni, quali il furto, danneggiamento, smarrimento, ecc., deve essere prontamente segnalato agli Organi di Polizia competenti ed alla Direzione Aziendale.

Gli Utenti interessati dalle disposizioni del presente regolamento, sono tenuti a contattare la Struttura del Sistema Informativo Aziendale prima di intraprendere qualsiasi attività tecnica non esplicitamente compresa nel presente documento, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Azienda.

Le risorse informatiche messe a disposizione o date in uso ad organizzazioni sono soggette ad accordi e condizioni contrattuali stipulate fra le parti.

Dati personali e/o sensibili non possono essere salvati sui supporti di memorizzazione locali dei *Personal Computer* a meno delle necessarie autorizzazioni e comunque previo l'utilizzo di adeguati sistemi di protezione (pseudonimizzazione, cifratura, ecc.).

4.2. Gestione ed assegnazione delle credenziali di autenticazione

L'accesso alle risorse informatiche aziendali (*Personal Computer*, reti locali, applicativi, base dati, ecc.) è vincolato all'utilizzo di credenziali personali (*username* e *password*). Le credenziali devono essere custodite dall'Utente con la massima diligenza e non devono essere comunicate a terze parti.

L'Azienda affida ad ogni Utente che ne abbia necessità le credenziali per l'accesso alle risorse di base del sistema informatico aziendale ed al sistema di posta elettronica ordinaria (di seguito anche solo "posta elettronica"); la robustezza e la validità temporale delle credenziali, nonché l'eventuale obbligo di modifica, è regolata dalla normativa vigente.

L'attribuzione, la modifica e la revoca delle credenziali di accesso ai sistemi è effettuata secondo processi standardizzati, l'attribuzione e la modifica delle credenziali e dei profili autorizzativi sono opportunamente tracciati. I profili autorizzativi concessi sono basati su schemi standard, gestendo solo successivamente eventuali eccezioni.

Ciascun Responsabile di struttura è tenuto a valutare la sussistenza dei requisiti per le autorizzazioni concesse agli Utenti: in caso di sopraggiunta necessità (ad esempio nel caso di conclusione del rapporto contrattuale, assegnazione ad altra Struttura, variazione nell'attività dell'Utente, ecc.) il Responsabile della Struttura deve darne tempestiva comunicazione alla Struttura del Sistema Informativo Aziendale.

Per alcuni profili contrattuali (es. Utenti con contratto di lavoro dipendente) in caso di cessazione del rapporto contrattuale sarà cura della Struttura della Gestione Risorse Umane darne tempestiva comunicazione formale alla Struttura del Sistema Informativo Aziendale secondo le modalità previste.

L'Azienda dispone di altri sistemi di autenticazione, tra i quali le smart card (Carta Operatore, Carta Nazionale dei Servizi/Tessera Sanitaria, LoginFVG), in possesso ed uso esclusivo dell'Utente assegnatario.

I profili autorizzativi concessi agli utenti devono essere periodicamente verificati dai responsabili delle strutture e dai referenti applicativi indicati all'interno del sistema aziendale di gestione delle credenziali al fine di garantire la continua consistenza dei livelli di protezione dei dati e delle informazioni.

Per maggiori informazioni e approfondimenti si fa riferimento alla procedura aziendale pubblicata nell'Intranet aziendale.

4.3. Utilizzo del Personal Computer

I *Personal Computer*, opportunamente configurati, consentono all'Utente di accedere alla rete dati dell'Azienda attraverso specifiche credenziali personali di autenticazione (di dominio *Microsoft Active Directory*).

Il Personale tecnico della Struttura del Sistema Informativo Aziendale e dei fornitori di servizi autorizzati ha la facoltà di collegarsi e visualizzare da remoto il *desktop* delle singole postazioni di lavoro al fine di garantire l'assistenza tecnica ed il supporto alla corretta attività operativa da parte degli Utenti. A tale scopo sono installati sui *Personal Computer* appositi *software* ("*agent*") per la rilevazione automatica della configurazione *hardware* e *software* delle postazioni di lavoro. L'intervento in teleassistenza viene effettuato su richiesta dell'Utente oppure in autonomia dal Personale tecnico della Struttura del Sistema Informativo Aziendale qualora siano riscontrati malfunzionamenti o violazione delle misure di sicurezza aziendali.

Il Personale tecnico della Struttura del Sistema Informativo Aziendale e dei fornitori di servizi autorizzati è autorizzato a compiere interventi sul sistema informatico aziendale nell'ottica di garantire la sicurezza e salvaguardia del sistema stesso, nonché per motivi tecnici e/o manutentivi di cui si evidenzi la necessità (ad es. aggiornamento/rimozione/implementazione di programmi, manutenzione *hardware,* ecc.). Detti interventi potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica ordinaria, nonché alla verifica sui siti *Internet* acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la continuità operatività dell'Azienda, si applica anche in caso di assenza prolungata o di impedimento dell'Utente, qualora non sia possibile procedere altrimenti.

L'Azienda vieta di memorizzare e/o trattare dati a fini personali di qualsiasi tipo per mezzo o all'interno degli strumenti aziendali concessi in uso: non potrà essere addotto come impedimento all'accesso delle risorse tecnologiche il fatto che siano presenti dati utilizzati a fini personali in forza del suddetto divieto di gestire dati non connessi alla propria mansione e/o attività istituzionale.

L'Utente che utilizza il *Personal Computer* s'impegna a mantenere la corretta configurazione della stazione di lavoro che utilizza e a non modificarla; non è consentito pertanto all'Utente variare le caratteristiche impostate sul *Personal Computer* in dotazione né procedere all'installazione di dispositivi di memorizzazione, comunicazione o altro (es. masterizzatori, modem, ecc.) senza il preventivo consenso della Struttura del Sistema Informativo Aziendale.

Non è consentita l'attivazione in autonomia di *password* di accensione (BIOS), senza preventiva autorizzazione da parte della Struttura del Sistema Informativo Aziendale.

Il *Personal Computer* deve essere, di norma, spento al termine dell'attività lavorativa allo scopo di preservarne la corretta funzionalità, di prevenire possibili problemi di sicurezza fisica e logica del sistema. L'Utente è tenuto a scollegarsi dal sistema o ad attivare il salvaschermo con *password* ogni qualvolta sia costretto ad assentarsi dalla postazione su cui opera: lasciare un *Personal Computer* incustodito e connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

L'Azienda ha avviato un percorso di progressiva introduzione di sistemi "*open source*" di automazione d'ufficio (es. *Libre Office*), pertanto sui *Personal Computer* di nuova fornitura saranno installate esclusivamente queste soluzioni applicative. Si precisa che le licenze di *MS Office* installate sui *Personal Computer aziendali*, o di qualsiasi altra soluzione software non fornita in ambito SIIR, sono esclusivamente quelle acquistate dall'Azienda.

4.4.Utilizzo dei Personal Computer portatili

L'Utente utilizzatore è responsabile del *Personal Computer* portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Il *Personal Computer* portatile non deve essere mai lasciato incustodito e sul disco fisso devono essere conservati solo i file strettamente necessari. Progressivamente sarà introdotta la funzionalità di crittografia del disco per tutti i *device* utilizzati in mobilità.

Ai *device* portatili si applicano le stesse regole di utilizzo previste per le Postazioni di Lavoro connesse alla rete aziendale.

L'Utente utilizzatore è tenuto ad eliminare definitivamente eventuali file, elaborati ed utilizzati, prima della riconsegna dello stesso al servizio a cui è assegnato.

Tutti i *Personal Computer* portatili devono collegarsi periodicamente (con frequenza almeno mensile) alla rete aziendale per consentire l'aggiornamento dell'antivirus, degli applicativi installati e del sistema operativo in conformità alle politiche di sicurezza adottate in Azienda.

4.5.Clear Screen Policy

Al fine di evitare che le infrastrutture informatiche (*Personal Computer*, *laptop*, ecc.) siano lasciate accessibili quando non presidiate, è necessario il rispetto delle seguenti regole da parte di tutto il personale dell'Azienda:

- se la postazione di lavoro portatile viene lasciata incustodita anche per brevi periodi deve essere ancorata tramite un apposito cavo di sicurezza ed è necessario attivare la funzione "blocca schermo" nel modo seguente: premere contemporaneamente i tasti *Ctrl_Alt_Canc* e successivamente il tasto *Enter/Invio* (oppure il tasto Windows in combinazione al tasto 'L');
- verificare sempre che lo schermo sia bloccato prima di allontanarsi dalla postazione di lavoro;
- se ci si allontana dalla postazione di lavoro per l'intera giornata e si è dotati di un dispositivo portatile, è necessario non lasciare incustodito il dispositivo portatile ed eventualmente assicurarsi che sia collocato in una opportuna locazione chiusa a chiave.

A completamento delle indicazioni di cui sopra, al fine di evitare eventi di *hacking visivo* e/o di utilizzo della Postazione di lavoro da parte di terzi, le politiche di sicurezza dell'Azienda prevedono comunque l'attivazione automatica del "blocca schermo" per inattività sulla Postazione di lavoro superiori ai 30'. Eventuali situazioni di eccezione saranno opportunamente valutate e condivise con la Direzione Strategica del Azienda.

4.6.Utilizzo di stampanti, multifunzioni, *fax*[1] *e fax-server*

È vietato l'utilizzo delle stampanti, fotocopiatrici, *device* multifunzione e *fax* aziendali per fini personali.

Stante il processo di progressiva dematerializzazione della Pubblica Amministrazione, si ricorda che la documentazione deve essere di norma creata, trattata e conservata nella sua forma originaria digitale, evitando di ricorrere alla stampa su carta.

Si raccomanda agli Utenti di prestare la massima attenzione alla stampa di documenti soprattutto nel caso si utilizzino stampanti di gruppo o accessibili a più persone. Il materiale stampato deve essere tempestivamente prelevato per evitare che possa essere visionato da personale non autorizzato. Al fine di aumentare la sicurezza aziendale le stampanti multifunzione saranno progressivamente dotate della imprescindibile funzione "*Follow me/Pool Printing"* che permette all'Utente, dopo aver lanciato la stampa verso una coda di stampa virtuale, di ottenere l'output a seguito di autenticazione tramite badge o password personale su una qualunque delle multifunzione presenti in rete anche in sedi fisiche diverse.

La stampa di documenti informatici dovrà essere limitata all'attività lavorativa e in ogni caso per documenti di cui esiste l'assoluta necessità di disporre della copia cartacea.

[1] Si ricorda che l'art. 47 "Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni", comma 2, lettera "c" del "CAD" recita: "[…] *È in ogni caso esclusa la trasmissione di documenti a mezzo fax*;"

Nell'utilizzare il *fax* in invio si deve prestare attenzione nella digitazione corretta del numero di telefono del destinatario prima di selezionare il tasto "invio", nell'attendere la stampa del rapporto di trasmissione e nel verificare la corrispondenza del numero di pagine da inviare con quelle effettivamente inviate.

È opportuno presidiare l'arrivo dei *fax* in ricezione in modo da evitare l'accesso ai documenti da parte di persone terze non autorizzate.

Nelle stampanti multifunzione, la scansione dei documenti potrebbe venir configurata come "*scan-to-mail"* e/o "*scan-to-disk*".

La modalità "*scan-to-mail*" consiste nell'invio del documento digitalizzato ad una casella di posta elettronica ordinaria. Le scansioni devono essere inoltrate alla propria casella di posta elettronica aziendale per verificarne la corretta scansione, e solo dalla propria casella si dovrà procedere all'inoltro a un destinatario terzo. Non è consentito l'invio di scansioni da multifunzione verso caselle di posta elettronica non aziendali. Nel caso di invio di allegati di grandi dimensioni è opportuno, dopo aver salvato il documento originato dalla scansione in allegato, cancellare la mail dalla posta in arrivo/partenza e successivamente dal cestino.

La modalità "*scan-to-disk*" consiste nel salvataggio del documento digitalizzato su cartella di rete condivisa. In tal caso, l'Utente si fa carico tempestivamente di spostare il file in una cartella non consultabile da Utenti non autorizzati alla visione del documento.

Deve essere posta la massima attenzione nella scansione di documenti contenenti dati personali e sensibili che deve avvenire, sotto la responsabilità dell'Utente, in ottemperanza alle normative vigenti.

4.7.Configurazione di sistema

Tutte le nuove postazioni di lavoro assegnate alle strutture sono configurate a partire da immagini *master* dei dischi che ottemperano le indicazioni previste dalle misure minime di sicurezza dettate dall'AgID.

Non è consentito modificare in alcun modo le configurazioni impostate sulle risorse dell'Azienda senza preventivo accordo con la Struttura del Sistema Informativo Aziendale.

Tutti i *Personal Computer* fissi aziendali devono essere collegati alla rete dati dell'Azienda affinché siano protetti da minacce esterne (*malware*) e non devono essere, per alcun motivo, scollegati dalla rete. Eventuali eccezioni devono essere esplicitamente autorizzate dalla Struttura del Sistema Informativo Aziendale.

4.8.Hardware e software

L'*hardware* e il *software* costituiscono l'ecosistema informativo dell'Azienda e possono essere acquisiti o accettati in donazione/comodato d'uso solo previa autorizzazione della Struttura del Sistema Informativo Aziendale che, nel caso di richieste da parte di terzi, esegue le opportune verifiche al fine di valutarne la compatibilità con le specifiche di sicurezza dell'Azienda, i sistemi in uso e l'infrastruttura di rete.

È fatto assoluto divieto all'Utente di intervenire in qualunque modo sull'*hardware* in dotazione. In caso di malfunzionamento delle apparecchiature assegnate, l'Utente s'impegna a seguire le modalità di attivazione del servizio di assistenza.

Non è consentito l'utilizzo di *hardware* di tipo personale salvo specifica autorizzazione della Struttura del Sistema Informativo Aziendale.

Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'Azienda o resi disponibili in ambito SIIR.

Non è altresì permessa la disinstallazione dei programmi, sia *software* di base che *software* applicativo. Interventi in tal senso possono essere effettuati, in caso di necessità, solo da parte dei tecnici della Struttura del Sistema Informativo Aziendale, sulla base di richiesta motivata da parte dell'Utente.

Non è consentita l'installazione, in autonomia, di *driver* per stampanti o per altri supporti come ad esempio masterizzatori, scanner, ecc.; in questo caso l'Utente dovrà richiedere alla Struttura del Sistema Informativo Aziendale di intervenire per effettuare l'installazione.

È facoltà della Struttura del Sistema Informativo Aziendale richiedere ad Insiel S.p.A., che gestisce l'infrastruttura del *proxy Internet* a livello regionale, di bloccare automaticamente il *download* di file potenzialmente infetti da siti non istituzionali o non affidabili. Nel caso in cui sia necessario "scaricare" file, anche gratuiti, dalla rete, l'Utente dovrà formulare una richiesta, preventivamente autorizzata dal Responsabile della propria Struttura, al Responsabile della Struttura del Sistema Informativo Aziendale, che, provvederà, previa eventuale verifica delle necessità e confronto con la Direzione strategica, ad autorizzare il *download* attraverso personale tecnico autorizzato ad effettuare direttamente l'installazione del programma.

L'Utente è responsabile del corretto utilizzo del *software* installato sulla propria postazione, sia *software* di base che *software* applicativo di vario genere; se ne raccomanda pertanto un uso diligente e consapevole.

Al fine di proteggere l'integrità del sistema informatico aziendale, gli Utenti non possono utilizzare *software* di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi *shareware* e/o *freeware*, eventuale *software* scaricato da *Internet* o proveniente da CD/DVD allegati a riviste e/o giornali o altro *software* posseduto a qualsiasi titolo.

La Struttura del Sistema Informativo Aziendale si riserva la facoltà di disabilitare in qualsiasi momento le interfacce USB delle stazioni di lavoro per impedire la possibilità di utilizzo di supporti di massa esterni, mezzi principali per l'introduzione di *malware* e di diffusione all'esterno di documenti contenenti dati personali e sensibili.

Non sono consentiti sia l'installazione sia l'utilizzo di strumenti *software* e/o *hardware* atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o di dati/documenti informatici.

La Struttura del Sistema Informativo Aziendale esegue periodicamente scansioni automatiche sui sistemi installati al fine di rilevare la presenza di *software* non autorizzato.

4.9. Aggiornamento del sistema operativo e del *software*

Gli aggiornamenti del *sistema operativo* sono necessari al fine di proteggere i *Personal Computer* e l'intera rete. In collaborazione con Insiel S.p.A., che governa il servizio, è stato implementato il *Windows Server Update Services* (WSUS) che effettua l'installazione degli aggiornamenti stabiliti in maniera automatizzata.

Gli aggiornamenti del *software* e dei *driver*, necessari al buon funzionamento della postazione di lavoro, saranno effettuati direttamente dai tecnici della Struttura del Sistema Informativo Aziendale attraverso l'impostazione di aggiornamenti automatici o intervenendo puntualmente a seguito della segnalazione dell'Utente.

4.10. Utilizzo e conservazione dei supporti removibili

Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti a controllo antivirus prima di essere aperti e/o utilizzati.

I supporti rimovibili (CD e DVD anche riscrivibili, supporti USB, hard disk ecc.) devono essere limitati a quelli strettamente indispensabili alle attività aziendali; in tali supporti non devono essere conservati, nemmeno provvisoriamente, file aziendali congiuntamente a file personali.

Non è permesso scaricare o copiare file contenuti in supporti removibili esterni (USB, hard disk drive, "chiavette USB", ecc..) se non attinenti alla propria attività lavorativa.

I supporti rimovibili contenenti dati personali devono essere ridotti ai casi di assoluta necessità ed inoltre, se non utilizzati, devono essere distrutti o resi inutilizzabili. I supporti magnetici rimovibili contenenti dati personali nonché informazioni costituenti il *know-how* aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto, o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o l'inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun Utente dovrà utilizzare gli strumenti messi a disposizione dal sistema operativo in uso per procedere alla formattazione completa e, se possibile, di basso livello, oppure alternativamente alla distruzione fisica.

Nel caso in cui dati, informazioni, immagini e/o notizie aziendali e/o dati riservati debbano essere salvati su supporti removibili, è obbligatorio conservare, custodire e controllare tali supporti affinché nessun soggetto terzo non autorizzato ne prenda visione o possesso o ne modifichi il contenuto. L'utente assegnatario è l'unico responsabile della custodia dei supporti e dei dati in essi contenuti.

I supporti rimovibili contenenti dati attinenti alle "categorie particolari" secondo il Regolamento UE 2016/679, nonché informazioni costituenti il know-how aziendale devono essere ridotti ai casi di assoluta ed estemporanea necessità e devono essere cifrati con password di adeguata robustezza; tali dispositivi devono essere custoditi dagli utenti con le medesime modalità imposte per la documentazione cartacea contenente la stessa tipologia di informazioni.

È assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Ogni Utente deve prestare la massima attenzione nell'utilizzo di memorie di massa esterne, in particolare nel caso in cui siano rilevati virus.

4.11. Utilizzo della rete fisica (LAN/WAN)

La rete fisica (LAN - *Local Area Network)* si basa sul protocollo TCP/IP (*Transmission Control Protocol/Internet Protocol*) ed è una risorsa strategica per l'Azienda in quanto connette ogni dispositivo informatico veicolando i dati conservati negli archivi centrali. Ogni disservizio relativo alla rete LAN può comportare notevoli disagi per l'operatività dell'Azienda.

Le reti LAN delle sedi aziendali operano interconnesse attraverso rete geografica aziendale (WAN - *Wide Area Network*).

Non è ammessa la connessione alla rete fisica aziendale di apparati atti ad effettuare connessioni con altre reti verso l'esterno (*router, switch, modem,* apparati *wireless*, ecc.).

L'uso di tali apparati, qualora necessario, dovrà essere autorizzato dalla Struttura del Sistema Informativo Aziendale. Analogamente non è ammesso l'utilizzo non autorizzato di dispositivi per la moltiplicazione di punti rete (*switch /mini switch*).

Viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro ed ogni altro dispositivo informatico (es. *Personal Computer* e portatili non aziendali) se non previa esplicita e formale autorizzazione della Struttura del Sistema Informativo Aziendale. Introdurre una macchina con un indirizzo IP (*Internet Protocol*) duplicato potrebbe causare gravi malfunzionamenti alla rete LAN.

È fatto assoluto divieto all'Utente di intercettare ed analizzare i pacchetti sulla rete aziendale, utilizzando analizzatori di rete sia *software* che *hardware*. Nel caso si riscontrasse la presenza di *Personal Computer* che generano traffico anomalo o che potrebbero far diminuire le prestazioni dell'intero sistema, sarà facoltà del personale tecnico della Struttura del Sistema Informativo Aziendale procedere all'interruzione anche immediata, se necessario, dell'attività di rete del *Personal Computer*.

È fatto divieto di svolgere attività che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli Utenti.

Non è consentito l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto. Non è consentito depositare materiale nelle vicinanze degli armadi di rete e nel raggio d'azione della porta di accesso all'armadio.

È obbligatorio interpellare la Struttura del Sistema Informativo Aziendale prima di ogni spostamento di postazioni informatiche, per valutarne l'impatto e la fattibilità e per predisporre le configurazioni adeguate.

4.12. Utilizzo della rete *Wireless* LAN (WLAN)

Ad integrazione della rete fisica, alcune aree dell'Azienda sono servite da collegamenti con tecnologia di trasmissione dati senza fili denominate *Wireless* LAN (WLAN).

Utilizzando apparati *access point* sono rese disponibili in alcune sedi aziendali due reti WLAN aventi SSID (*Service Set IDentifier* - nome con cui la rete senza fili si identifica agli Utenti) differenziati, uno di tipo *enterprise* e uno di tipo *guest*.

La rete WLAN di tipo *enterprise* risulta a tutti gli effetti un'estensione della rete LAN aziendale, pertanto, i dispositivi connessi avranno la possibilità di accedere alle medesime risorse della rete locale fisica. È vietata la connessione alla rete *enterprise* di sistemi diversi dai portatili aziendali (es. attraverso *laptop*, *tablet* e/o cellulari personali).

La rete WLAN di tipo *guest* è separata logicamente dalla rete LAN aziendale e fa riferimento ad un servizio messo a disposizione agli Ospiti/Degenti/Dipendenti, a cui si può collegare un dispositivo di tipo "Personale". La navigazione *Internet* è libera, previa autenticazione svolta seguendo le modalità indicate nella pagina di accesso.

Non è ammessa la connessione alla rete WLAN aziendali di apparati atti ad effettuare connessioni con altre reti verso l'esterno.

4.13. Dominio e autenticazione

In Azienda è attiva una configurazione basata su dominio *Microsoft Active Directory*. La Struttura del Sistema Informativo Aziendale si occupa della creazione, cancellazione e modifica degli *account* (Utenti, Computer, Gruppi, Unità organizzative, ecc.) sulla base di specifiche esigenze/richieste, alla gestione ed implementazione di criteri in accordo con le normative vigenti per il tramite di Insiel S.p.A..

All'atto dell'assunzione, tutti gli Utenti, dipendenti a tempo determinato/indeterminato dell'Azienda, vengono dotati di credenziali di accesso al dominio e di un indirizzo di posta elettronica istituzionale, da utilizzare per scopi legati al rapporto di lavoro con l'Azienda.

Gli eventi relativi agli accessi alle postazioni aziendali vengono registrati per un periodo limitato di tempo sulle postazioni medesime dalle funzioni del sistema operativo e nei diversi *Domain Controller*, e da questi possono essere inviati ai sistemi di *Security Information and Event Management* (SIEM). In questi ultimi possono essere raccolti anche i dati di accesso ai principali apparati di rete e ai server *Radius* aziendali. Tali dati vengono conservati al fine di rispondere ad eventuali richieste da parte dell'Autorità Giudiziaria, dell'Autorità di Pubblica Sicurezza e del Garante.

4.14. Accesso ad applicazioni e banche dati

In relazione agli applicativi aziendali, la Struttura del Sistema Informativo Aziendale fornisce le credenziali di accesso ai singoli operatori ed assegna i profili d'uso in coerenza alle richieste pervenute dai Responsabili delle strutture. È onere dei Responsabili delle strutture comunicare tempestivamente qualsiasi modifica relativa all'organico in carico che richieda la sospensione e/o la revoca dell'autorizzazione all'accesso alle risorse informatiche e alle banche dati.

Gli eventi relativi agli accessi alle applicazioni e alle banche dati possono essere registrati lato applicativo ed eventualmente da questi inviati ai sistemi di *Security Information and Event Management* (SIEM). Tali dati vengono conservati al fine di rispondere ad eventuale legittima richiesta da parte dell'Autorità Giudiziaria, dell'Autorità di Pubblica Sicurezza e del Garante.

4.15. Unità di rete, memorizzazione file e *backup*

Le unità di rete sono le rappresentazioni del sistema di memorizzazione dei file (*file server*) dell'Azienda. Agli Utenti del dominio aziendale è prevista l'assegnazione di una cartella per il salvataggio dei file su unità di rete.

I dischi o le altre unità di memorizzazione locali (es. il disco rigido della propria postazione di lavoro) non sono soggette al salvataggio, pertanto si esorta a non memorizzare informazioni in tali dispositivi. La responsabilità del salvataggio degli eventuali dati ivi contenuti è a carico del singolo Utente.

Le cartelle di rete sono aree di condivisione di informazioni strettamente professionali e non devono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file non sia legato all'attività lavorativa non può essere dislocato, nemmeno temporaneamente, in queste unità.

I livelli di condivisione/privilegi di lettura e scrittura o di sola lettura delle cartelle vengono definiti dal/dai Responsabile/i della/e struttura/e proprietaria/e delle cartelle stesse e pertanto dei documenti ivi contenuti.

Non è consentita la modifica dei permessi di accesso delle cartelle di rete da parte degli Utenti.

Ove possibile, la Struttura del Sistema Informativo Aziendale metterà a disposizione degli Utenti una cartella di rete a seguito di richiesta specifica fatta dal Responsabile di struttura. L'Utente potrà utilizzare in maniera esclusiva e riservata tale unità per il salvataggio dei dati comunque di interesse aziendale.

Alla data di conclusione del rapporto di lavoro dell'Utente con l'Azienda, la Struttura della Gestione Risorse Umane notificherà la cessazione del rapporto di lavoro alla Struttura del Sistema Informativo Aziendale. Salvo specifiche richieste e/o casi particolari che saranno opportunamente trattati, la Struttura del Sistema Informativo Aziendale potrà procedere alla variazione dei permessi di accesso alla stessa a favore del Responsabile della struttura di afferenza dell'Utente come previsto dalla normativa vigente.

Nel caso di cessazione del rapporto di lavoro (mobilità in uscita, pensionamento, dimissioni o decesso), trascorsi 30 giorni dalla comunicazione, la Struttura del Sistema Informativo Aziendale procederà alla cancellazione definitiva della cartella di rete assegnata in modalità esclusiva e non sarà possibile recuperare i dati in essa contenuti.

Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi da parte degli Utenti, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è assolutamente da evitare un'archiviazione ridondante.

È assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Nel caso vengano attuati trattamenti idonei a rivelare lo stato di salute o la vita sessuale dei soggetti è onere del Responsabile di struttura l'adozione degli strumenti messi a disposizione al fine di applicare opportune tecniche di cifratura atte a rendere non accessibili le informazioni trattate.

4.16. Antivirus

L'Azienda utilizza il servizio antivirus fornito in ambito *SIIR* costituito, allo stato dell'arte, da un sistema antivirus *client/server* basato su *agent* distribuito e gestito centralmente.

La politica di sicurezza aziendale prevede l'installazione su tutte le postazioni di lavoro dell'*agent* che è oggetto ad aggiornamento automatico periodico. Non è ammesso l'utilizzo di sistemi antivirus diversi, se non espressamente autorizzati dalla Struttura del Sistema Informativo Aziendale. I *Personal Computer* eventualmente *off-line* si aggiornano non appena vengono ricollegati alla rete dati (di norma alla prima accensione).

Ogni Utente è tenuto a controllare la presenza del *software* antivirus verificandone la presenza dell'icona sul *system tray* del *desktop* della propria Postazione di lavoro. Nell'eventualità si riscontrasse la mancanza di tale *software* l'Utente dovrà darne tempestiva segnalazione alla Struttura del Sistema Informativo Aziendale per attivare le successive azioni inerenti all'installazione.

Nel caso il *software* antivirus rilevi la presenza di un virus che non è riuscito ad eliminare, l'Utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il Computer;
- segnalare l'evento all'*help-desk*.

Ogni dispositivo di memorizzazione esterno, o di provenienza non certa, dovrà essere verificato a cura dell'Utente, mediante il programma antivirus prima del suo utilizzo. Qualora venga rilevata un'infezione non eliminabile dal sistema antivirus, il dispositivo non dovrà essere utilizzato e immediatamente scollegato.

L'*agent* antivirus installato sulle postazioni di lavoro è normalmente configurato con attiva la funzione per svolgere la scansione di tutte le periferiche rimovibili che vengono collegate al Personal Computer. È inoltre normalmente attivo il blocco dell'"*autorun*" che impedisce l'esecuzione automatica di contenuti al momento della connessione al *Personal Computer* dei dispositivi mobili.

Qualora l'Utente riscontrasse una configurazione differente rispetto a quanto sopra indicato è tenuto a segnalarlo prontamente all'*help-desk* di assistenza.

4.17. Valutazione del rischio relativo alla sicurezza delle informazioni

Al fine di facilitare e rendere tempestive le operazioni di aggiornamento del *software*, oltre che per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, i tecnici informatici addetti all'assistenza (in qualità di Amministratori di Sistema) possono avvalersi di strumenti di controllo remoto che consentano di compiere le necessarie operazioni attraverso la rete locale o un collegamento interno protetto (VPN).

Sui dispositivi informatici aziendali sono installati opportuni *agent* che consentono, fra le altre:

- l'accesso remoto al *desktop* Utente, configurato in modo che l'Utente sia comunque consapevole dell'intervento tecnico in corso e lasciando all'Utente stesso l'approvazione dell'avvio dell'azione a meno di accordi diversi; la durata del collegamento, che è tracciato in appositi file di log, è limitata al tempo strettamente necessario all'esecuzione dell'intervento tecnico;
- la rilevazione delle vulnerabilità (*Vulnerability Detection*), ovvero delle debolezze insite nei sistemi informativi e che, se sfruttate, potrebbero esporre l'azienda a rischi informatici;
- l'identificazione delle minacce (*Threat Detection*), ovvero degli eventi in grado di sfruttare una vulnerabilità per provocare un danno all'azienda;
- l'utilizzo degli elementi raccolti nelle attività precedentemente descritte per identificare e valutare le contromisure esistenti (*Threat &Vulnerability Assessment*);
- la definizione delle liste di azioni correttive da poter applicare per mitigare i rischi informativi a cui l'azienda è esposta (*Control Selection*);
- la rilevazione della presenza sulle Postazioni di Lavoro di tipologie di esportazioni di dati e/o informazioni riservate non protette dalle necessarie misure di sicurezza che potrebbero comportare rischi per l'Azienda in caso di furto delle apparecchiature, esfiltrazione di dati e/o di contenuti informativi, attraverso strumenti di *Data Loss Prevention* (DLP).

L'Amministratore del Sistema, per l'espletamento delle sue funzioni (es. salvataggio e ripristino di archivi, tutela della sicurezza informatica, ecc.), ha la facoltà, in qualunque momento, di accedere, nel rispetto della normativa vigente, ai dati trattati da ciascun Utente, ivi compresi gli archivi di posta elettronica ordinaria.

L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza sia sulle unità locali delle postazioni informatiche degli incaricati sia sulle unità a dischi di rete.

4.18. Accesso degli Utenti esterni

I fornitori di servizi autorizzati che effettuano manutenzioni da remoto agli applicativi o ai *server* (teleassistenza), accedono come utenti esterni alla rete aziendale attraverso un accesso VPN protetto da *firewall* gestito da Insiel S.p.A..

Il personale tecnico del Sistema Informativo predispone la modulistica specifica, sulla base delle informazioni ricevute dalla ditta che intende attivare la teleassistenza, la trasmette compilata a Insiel S.p.A. affinché svolga la configurazione di conseguenza. Le abilitazioni, con relative credenziali di accesso, sono fornite dalla Struttura del Sistema Informativo Aziendale in busta chiusa Personale ad un referente indicato dalla ditta. Le utenze sono nominali ed inserite sull'albero di *Microsoft Active Directory* dell'Azienda in unità organizzative dedicate o sui *server Radius* di Insiel S.p.A..

4.19. Mobile computing/teleworking

Al personale cui è concessa, previo processo autorizzativo, la facoltà di lavorare dall'esterno dell'Azienda sono forniti opportuni strumenti di autenticazione anche con complessità maggiore rispetto allo standard aziendale (meccanismi di *strong authentication*). Per le attività operative svolte in perimetro esterno all'Azienda devono essere garantiti opportuni livello di protezione degli *asset* che ricomprendo, fra le altre:

- l'attenzione a non fornire informazioni e comunicazioni in luoghi pubblici e affollati, moderando le informazioni trattate oralmente;
- la protezione degli asset da sottrazioni fisiche (furti) e/o smarrimenti, adottando misure quali utilizzo sistematico di armadi chiusi a chiave, di cavi di sicurezza.

4.20. *Internet* e navigazione

L'abilitazione alla navigazione è assegnata a livello di singola utenza ed è uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

L'abilitazione alla navigazione *Internet* deve essere richiesta ed autorizzata dal Responsabile della struttura, a cui afferisce l'Utente, ed inviata alla Struttura del Sistema Informativo Aziendale.

Agli Utenti non abilitati alla navigazione *Internet* è fatto divieto assoluto di connettersi alla rete Internet. È fatto altresì divieto di utilizzare credenziali di accesso ad *Internet* diverse da quelle di cui si è assegnatari.

L'Utente è direttamente responsabile, civilmente e penalmente (a norma delle vigenti leggi) per l'utilizzo del servizio Internet. La responsabilità si estende anche alla violazione degli accessi protetti, del *copyright* e delle licenze d'uso.

È assolutamente vietata la navigazione *Internet* per motivi diversi da quelli strettamente legati all'attività lavorativa. A titolo puramente esemplificativo, l'Utente non potrà utilizzare *Internet* per:

- l'*upload* o il *download* di *software* (anche se gratuiti, freeware, shareware, …), nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività

lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il Personale della Struttura del Sistema Informativo Aziendale);

- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking*, acquisti *on-line* e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Aziendale;
- il *download* di file, del tipo audio-video, e/o altri tipi di file o programmi per la fruizione di contenuto non legati ad un uso d'ufficio;
- le ricerche e/o consultazioni di siti il cui contenuto informativo appaia osceno, offensivo alla morale nonché alla pubblica decenza, a contenuto discriminatorio di taluni o razzista, a sfondo politico e/o religioso;
- la diffusione di *malware* o altri programmi, la cui azione consista nel sabotaggio, distruzione o alterazione del contenuto informativo dei dispositivi informatici aziendali e dei dati in essi contenuti, anche qualora l'obiettivo sia all'esterno della rete aziendale;
- la registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a forum non professionali, l'utilizzo di *chat line*, di *social network* e bacheche;
- la cessione/fornitura di dati di altri Utenti, organismi e/o aziende;
- l'attività di pirateria informatica in generale.

L'Azienda, per il tramite di Insiel S.p.A. che governa tale tecnologia, regolamenta la navigazione *Internet* attraverso l'utilizzo di sistemi di *web filtering* che inibiscono, preventivamente, l'accesso a siti dal contenuto chiaramente non attinente alle attività istituzionali, contrario al buon costume, potenzialmente pericoloso per la sicurezza e l'integrità dei dispositivi e dei servizi informatici aziendali.

La Struttura del Sistema Informativo Aziendale, qualora autorizzato della Direzione Generale, ha facoltà di porre limiti alla ricerca di contenuti *Internet* escludendo dalla navigazione, siti non attinenti agli scopi aziendali. Il sistema di navigazione per mezzo di *proxy Internet* esegue il monitoraggio dei siti visitati dagli Utenti. Tali dati vengono conservati al fine di rispondere ad eventuale legittima richiesta da parte dell'Autorità Giudiziaria, dell'Autorità di Pubblica Sicurezza e del Garante.

4.21. Posta elettronica

La casella di posta elettronica ordinaria assegnata all'Utente è uno strumento di lavoro di proprietà aziendale concesso in utilizzo al fine di un più proficuo svolgimento della prestazione lavorativa. Al momento dell'assunzione l'Utente, dipendente a tempo determinato/indeterminato dell'Azienda, viene dotato di credenziali di accesso alla rete aziendale e di una casella di posta elettronica ordinaria (PEO) nominale istituzionale.

Su richiesta dei Responsabili di Struttura sono definite caselle di posta elettronica ordinaria di servizio (es. di ufficio, di servizio, di progetto) a cui vengono associate, sempre su richiesta del Responsabile di Struttura, una o più utenze di accesso nominali.

È buona norma che le caselle di posta elettronica nominali e "di ufficio/servizio/progetto" siano consultate con cadenza almeno giornaliera.

Qualora l'Utente debba allontanarsi dalla propria postazione di lavoro, al fine di impedire l'accesso da parte di terzi, è tenuto a terminare l'accesso alla consultazione della casella di posta elettronica ordinaria.

È vietato altresì l'accesso a caselle di posta aziendali diverse da quelle assegnate.

L'accesso alle caselle di posta elettronica aziendale avviene per mezzo di un portale *webmail* utilizzando le credenziali che coincidono con quelle per l'accesso alla rete aziendale. Il portale *webmail* è fruibile via Internet, quindi anche al di fuori della rete aziendale.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Ogni Utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o altro codice *malware*. È buona norma, ad esempio, non aprire mail o relativi allegati sospetti. È obbligatorio porre la massima attenzione nell'aprire i file in allegato ai messaggi di posta elettronica prima del loro utilizzo, non eseguire *download* di file eseguibili o documenti da siti non conosciuti.

La casella di posta elettronica ordinaria ha una dimensione finita prestabilita. È compito dell'Utente mantenere la casella di posta in ordine, cancellando documenti inutili e soprattutto allegati, in particolare quelli di grosse dimensioni, che alla lunga possono esaurire lo spazio disponibile. Si raccomanda di svuotare periodicamente il cestino che raccoglie i messaggi cancellati.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo e non esaustivo, l'Utente non potrà utilizzare la posta elettronica per:

- inviare e/o ricevere allegati contenenti filmati o brani musicali non legati all'attività lavorativa;
- inviare e/o ricevere messaggi personali o per partecipare a dibattiti, aste *on line*, concorsi, *forum* o *mailing-list*;
- partecipare a catene telematiche (o di Sant'Antonio) e, a riguardo, non si dovrà in alcun caso procedere nemmeno all'apertura degli allegati contenuti in tali messaggi;
- aprire mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro);
- rispondere a messaggi provenienti da un mittente sconosciuto o aventi contenuto dubbio, in quanto tale atto assicura al mittente l'esistenza del destinatario;
- comunicare informazioni riservate, dati personali e/o dati critici, senza garantirne l'opportuna protezione;
- inviare, in modo intensivo, posta elettronica indesiderata o invasiva (spam).

È possibile ottenere, nelle comunicazioni aziendali esterne ed interne, una segnalazione relativamente al recapito del messaggio e all'avvenuta lettura; si ricorda però che la conferma dell'avvenuta lettura è a discrezione del destinatario. Per avere garanzia di avvenuto ricevimento è pertanto necessario chiedere al destinatario risposta con conferma esplicita.

Si raccomanda di prestare attenzione alla dimensione degli allegati, poiché il gestore di posta blocca i messaggi (in ingresso ed in uscita) la cui dimensione ecceda 20 MB (*Mega Byte*). È pertanto consigliato, nel caso di invii di documenti di gradi dimensioni, l'utilizzo di formati compressi (es. zip).

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati nel rispetto del principio di necessità e di proporzionalità, è opportuno che l'Utente attivi in caso di assenze programmate (es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) messaggi di risposta automatica per avvisare il mittente.

Come previsto dal Provvedimento del Garante, "…in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile …".

In caso di assenza non programmata (dovuta ad esempio a "malattia"), qualora non sia possibile acquisire ordinariamente informazioni o comunicazioni che, se non ricevute o recepite con ritardo, potrebbero arrecare un evidente danno all'Azienda, e nel caso non sia stato individuato il fiduciario nelle modalità sopra descritte, sarà consentito al superiore gerarchico dell'Utente (Responsabile di struttura) di accedere alla casella di posta elettronica dell'Utente.

Il Responsabile di struttura, attraverso una richiesta scritta inviata alla Struttura del Sistema Informativo Aziendale, verrà abilitato all'accesso a detta casella di posta. Alla prima occasione utile, il Responsabile di struttura deve informare l'Utente interessato dell'attività svolta utilizzando la casella di posta elettronica nominale assegnata. Tale tipologia di accesso deve essere formalmente motivata e sottoscritta dal Responsabile della struttura. Il provvedimento di cui sopra e il verbale delle operazioni eseguite sono consegnati all'Utente al momento del suo rientro in servizio.

Il personale tecnico della Struttura del Sistema Informativo Aziendale potrà accedere alla casella di posta elettronica per le sole finalità atte a garantire la sicurezza e la salvaguardia del sistema, nonché per motivi tecnici e/o manutentivi.

L'Azienda, per il tramite di Insiel S.p.A. che gestisce il sistema di posta elettronica aziendale, ha facoltà di accesso ai *file* di *log*. I servizi di posta elettronica sono suscettibili di controlli che possono arrivare fino alla conoscenza, da parte del datore di lavoro, del contenuto della corrispondenza (attraverso la tenuta di *log file,* del monitoraggio del traffico mail e dell'archiviazione dei messaggi). I dati e la corrispondenza intercorsa sono mantenuti riservati e possono essere resi disponibili a fronte di legittima richiesta da parte dell'Autorità Giudiziaria, dell'Autorità di Pubblica Sicurezza e del Garante.

Nei giorni antecedenti all'interruzione del rapporto di lavoro, a causa cessazione (es. mobilità in uscita, pensionamento, dimissioni) o sospensione (es. aspettativa a vario titolo, congedi, in utilizzo/comando presso altri enti) è onere dell'assegnatario della casella di posta elettronica inserire idoneo messaggio di risposta automatica pertinente con la disattivazione della casella.

La Struttura della Gestione delle Risorse Umane notificherà l'interruzione del rapporto di lavoro alla Struttura del Sistema Informativo Aziendale che, salvo diverse indicazioni, specifiche richieste e casi particolari che verranno opportunamente trattati, procederà con la disabilitazione dell'utenza associata alla casella di posta (impedendone l'accesso) e con l'inibizione dell'invio e della ricezione di messaggi.

In caso di sospensione del rapporto di lavoro, verrà valutata di concerto dal Responsabile di struttura da cui dipende il soggetto interessato o la Direzione Strategica dell'Azienda, l'opportunità di procedere alla cancellazione o alla sospensione della casella di posta elettronica Personale.

La cancellazione delle caselle di posta elettronica di servizio/progetto/ufficio avviene su specifica richiesta del Responsabile di struttura che ha in carico la gestione della casella stessa.

Le caselle di posta elettronica disattivate restano inutilizzabili, ma a disposizione per altri 12 mesi, solo al fine di rispondere ad eventuale legittima richiesta da parte dell'Autorità Giudiziaria, dell'Autorità di Pubblica Sicurezza e del Garante.

4.22. Sistemi di controllo graduali, verifiche e sanzioni Spam e *phishing*

Qualora si ravvisassero casi presunti di *spam* o di *phishing*, è necessario segnalarli immediatamente a Insiel S.p.A. La segnalazione deve avvenire allegando il messaggio interessato in una nuova mail da inviare alla casella dedicata antispam@insiel.it, specificando nell'oggetto la dicitura "*Spam non fermato*".

4.23. Sistemi di controllo graduali, verifiche e sanzioni

È fatto obbligo a tutti gli Utenti di osservare le disposizioni del presente regolamento.

L'Azienda si riserva la possibilità di compiere controlli mirati sull'uso delle risorse informatiche al fine di verificare l'effettivo e corretto adempimento della prestazione lavorativa, nel rispetto della libertà e della dignità degli Utenti nonché della normativa sulla protezione dei dati personali.

Qualora le misure indicate nel presente regolamento non fossero sufficienti ad evitare comportamenti anomali, il Personale della Struttura del Sistema Informativo Aziendale (o Insiel S.p.A. per conto della Struttura del Sistema Informativo Aziendale) procederà con delle verifiche con granularità sempre più fine, a livello di Struttura, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole.

Perdurando la situazione anomala, tali controlli, nelle forme e per le motivazioni di cui sopra, potranno essere effettuati su base individuale; all'esito degli stessi potrà essere avviato, nei confronti dell'Utente interessato, regolare procedimento disciplinare nelle forme e nei modi sanciti dalla normativa vigente e dal CCNL applicato.

Tutti gli Utenti sono tenuti a segnalare alla Direzione Aziendale prontamente qualsiasi violazione al presente regolamento in forma non anonima. Viene comunque tutelato dall'Azienda il diritto alla *privacy* degli Utenti che comunicassero dette violazioni nei limiti previsti dalla normativa italiana.

4.24. Uso Personale di strumenti aziendali

Non sono previste modalità di utilizzo Personale di risorse informatiche dell'Azienda con pagamento o fatturazione a carico dell'Utente.

4.25. Trattamento dei dati del personale

I trattamenti dei dati degli Utenti, previsti dal presente regolamento, sono finalizzati unicamente alla corretta e completa gestione e relativo controllo dell'utilizzo delle risorse informatiche; il conferimento dei dati personali è necessario ai fini dello svolgimento di tali attività. L'eventuale rifiuto comporta l'impossibilità dello svolgimento del rapporto di lavoro. Le operazioni di trattamento sono effettuate in modalità cartacea ed informatizzata dal Personale incaricato degli uffici competenti nei limiti necessari per perseguire le sopra citate finalità.

4.26. Disposizioni finali, entrata in vigore e pubblicità

Il regolamento per l'utilizzo delle risorse informatiche entra in vigore dalla data di esecutività del relativo decreto di adozione.

Con l'entrata in vigore del regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Per quanto non espressamente previsto sarà fatto riferimento alla normativa vigente in materia.

Il regolamento verrà portato a conoscenza di tutti gli Utenti dell'Azienda attraverso la pubblicazione sul sito *Internet* aziendale, inoltre verrà pubblicata su una unità di rete accessibile a tutti gli utilizzatori e verrà inoltrata nota informativa a tutte le strutture aziendali.

È fatto obbligo di adeguare i propri comportamenti alle disposizioni previste nel presente regolamento ed a chiunque competa di osservarle.

4.27. Riferimenti allo Standard ISO27001:2013 e Misure minime di sicurezza ICT

L'applicazione del presente documento contribuisce alla realizzazione dei seguenti requisiti dello standard ISO 27001:2013:

- A.5. Politica per la sicurezza delle informazioni
- A.6 Organizzazione della sicurezza delle informazioni
- A.7 Sicurezza delle risorse umane
- A.8 Gestione degli asset
- A.9 Controllo degli accessi
- A.10 Crittografia
- A.11 Sicurezza fisica e ambientale
- A.12 Sicurezza delle attività operative
- A.13 Sicurezza delle comunicazioni
- A.14 Acquisizione, sviluppo e manutenzione dei sistemi
- A.15 Relazioni con i fornitori
- A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni
- A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa
- A.18 Conformità.

Contribuisce inoltre alla realizzazione dei seguenti requisiti delle "Misure minime di sicurezza ICT":

- ABSC 1 (CSC 1): Inventario dei dispositivi autorizzati e non autorizzati
- ABSC 2 (CSC 2): Inventario dei software autorizzati e non autorizzati
- ABSC 3 (CSC 3): Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop., workstation e server

- ABSC 4 (CSC 4): Valutazione e correzione continua delle vulnerabilità
- ABSC 5 (CSC 5): Uso appropriato dei privilegi di amministratore
- ABSC 8 (CSC 8): Difese contro i malware
- ABSC 10 (CSC 10): Copie di sicurezza
- ABSC 13 (CSC 13): Protezione dei dati

4.28. Revisione del documento

Si procederà all'aggiornamento del documento ogni qualvolta si verifichi almeno una delle seguenti condizioni:

- identificazione di nuovi rischi o minacce/modifiche rispetto a quanto considerato in una precedente attività di analisi del rischio;
- incidenti di sicurezza correlati al patrimonio informativo che l'Azienda intende tutelare, appartenenti cioè all'ambito del Sistema di Gestione della Sicurezza Informatica;
- evoluzione del contesto normativo e legislativo in materia di sicurezza;
- risultati di analisi sui costi, sugli impatti e sull'efficacia e sull'efficienza del sistema di gestione per la sicurezza delle informazioni;
- eventuali ulteriori indicazioni derivanti dalle funzioni di *assurance* a supporto dell'Azienda.

5. Terminologie e abbreviazioni

access point: è un dispositivo elettronico di telecomunicazioni che, collegato ad una rete cablata, o anche ad un router permette all'utente mobile di accedervi in modalità *wireless* direttamente tramite il suo terminale, se dotato di scheda *wireless*;

account: insieme di funzionalità, strumenti e contenuti attribuiti ad un nome Utente in determinati contesti operativi, non solo in siti *web* o per usufruire di determinati servizi su *Internet* ma anche per accedere alle applicazioni *software*;

agent: un'applicazione installata sul Computer dell'Utente che si connette ad un processo *server*. Esempi di *user agent* sono i *browser web,* i lettori multimediali e i programmi client (*Mail User Agent*) come *Outlook*;

active directory: insieme di servizi di rete adottati dai sistemi operativi Microsoft a partire da Windows 2000 Server e gestiti da un *domain controller*;

autenticazione informatica*:* è il processo attraverso il quale viene verificata l'identità di un utente che vuole accedere ad un computer, ad una rete, in generale ad una risorsa informatica;

backup: indica la replicazione su un qualunque supporto di memorizzazione di materiale informativo archiviato nella memoria di massa dei Computer, siano essi *Personal Computer, workstation, server, tablet, smartphone, ecc.* al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali;

banca dati o base dati*:* qualsiasi complesso organizzato di dati, ripartito in una o più unità dislocate in uno o più sistemi;

comunicazione elettronica*:* qualsiasi comunicazione creata, inviata, inoltrata, trasmessa, archiviata, copiata, scaricata, mostrata, vista o stampata da uno o più sistemi o servizi di comunicazione elettronica;

sistema di autenticazione*:* le informazioni e/o i dispositivi, in possesso di una persona, solo da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

dati personali*:* qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra

domain controller: è un *server* che, nell'ambito di un dominio Microsoft Windows attraverso i servizi messi a disposizione da *Active Directory*, organizza la struttura del dominio in termini di utenti, gruppi, regole, *Computer*, stampanti, risorse di rete, ecc. e gestisce le richieste di autenticazione per la sicurezza (*login*, controllo dei permessi, ecc.);

dominio Microsoft Windows: un insieme di Computer che condividono un archivio (*directory*) di risorse informatiche e che vengono amministrati attraverso regole e procedure comuni;

download: scaricamento, l'azione di ricevere o prelevare da una rete telematica (es. da un sito *web*) un file, trasferendolo sulle unità di memorizzazione del Computer;

driver: insieme di procedure *software*, che permettono ad un sistema operativo di governare un dispositivo *hardware*;

enterprise: aziendale, o rivolto ad utenti aziendali;

***fax**:* apparato telefonico per la trasmissione (invio e ricezione) di immagini fisse, tipicamente copie di documenti;

fax-server: sistema installato in un *server* di rete locale (LAN) che consente agli Utenti, i cui *Computer* sono collegati alla LAN, di inviare e ricevere messaggi *fax*;

firewall: un dispositivo *hardware/software* per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi;

freeware: una categoria di *software* proprietario il cui utilizzo è concesso a titolo gratuito;

***Garante per la protezione dei dati personali**:* l'autorità di cui all'art.153 del Codice Privacy, "Il Garante" istituita dalla Legge n.675 del 31/12/1996;

***guest*:** ospite, rivolto ad utenti ospiti;

hacking visivo: è l'insieme di situazioni per cui un malintenzionato può sfruttare la visuale, fisicamente o telematicamente intesa, del desktop del *Personal Computer* della vittima, con il fine ultimo di rubare informazioni sensibili, credenziali o la stessa immagine del dipendente;

immagine master: copia di un disco che viene solitamente utilizzata come punto di partenza per installare *Personal Computer* di caratteristiche analoghe;

intranet: un sistema di comunicazione interno all'azienda basato su tecnologia web e su cartelle in condivisione,

know-how aziendale: identifica le conoscenze e le abilità operative necessarie per svolgere una determinata attività lavorativa;

laptop/notebook: è un piccolo Personal Computer portatile con un fattore di forma "a conchiglia", con in genere un sottile schermo LED montato all'interno del coperchio superiore e una tastiera alfanumerica all'interno del coperchio inferiore;

malware: *malicious-software* (che significa letteralmente *software* malintenzionato, ma di solito tradotto come *software dannoso*), indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un *Computer*, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata;

mini switch: rappresenta un dispositivo di rete di piccole dimensioni che funge da nodo di smistamento dati di una rete di comunicazione;

***password**:* detta *parola chiave,* parte della credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri alfanumerici o altri dati in forma elettronica;

phishing: tipo di truffa effettuata via *Internet* attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un soggetto affidabile in una comunicazione;

***proxy Internet**:* un sistema informatico intermedio che fa da filtro tra utente e *Internet*, con la funzione di identificare l'Utente e di accelerare/inibire, secondo i casi, l'accesso a determinati destinazioni e siti *Internet*;

remote banking: l'insieme di servizi offerti dalle banche per via telematica o telefonica ai propri clienti;

***responsabile**:* la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali;

***responsabile della Struttura del Sistema Informativo Aziendale**:* il responsabile della gestione delle risorse informatiche aziendali;

***risorse informatiche aziendali**:* qualsiasi combinazione di apparati tecnologici di un'azienda e del Sistema Sanitario Regionale, *hardware* o *software*, utilizzati per le comunicazioni elettroniche ed elaborazione dei dati;

scanner: è una periferica in grado di acquisire in modalità ottica una superficie analogica (fogli stampati, pagine, fotografie, diapositive), di interpretarla come un insieme di *pixel*, e quindi di ricostruirne la copia fotografica sotto forma di immagine digitale;

***server**:* è un *Personal Computer* dedicato, che eroga servizi e risorse in una rete locale di Personal Computer;

server Radius: è un server utilizzato per gestire le funzioni di autenticazione (*authentication*), controllo degli accessi (*authorization*) e tracciamento del consumo delle risorse da parte degli utenti (*accounting*) nell'ambito dell'accesso alle VPN;

shareware: è una tipologia di licenza *software* molto popolare sin dai primi anni novanta. Vengono distribuiti sotto tale licenza in genere programmi facilmente scaricabili via *Internet* o contenuti in e CD e DVD quasi sempre allegati alle riviste di informatica;

***servizi informatici aziendali**:* l'insieme dei servizi informatici erogati attraverso le *risorse informatiche aziendali*, che consentono all'Utente di accedere, visualizzare, modificare, e compiere ogni altra operazione su dati a qualunque titolo memorizzati nei dispositivi informatici aziendali, o da questi accessibili, nonché gli eventuali servizi ausiliari al loro funzionamento;

software: l'insieme dei programmi che possono essere impiegati su un sistema di elaborazione dei dati;

spam: detta anche posta indesiderata, messaggio di posta elettronica, in genere con contenuto pubblicitario, che giunge indesiderato a una moltitudine di destinatari contemporaneamente riempiendo inutilmente le loro caselle di posta elettronica;

***strumenti elettronici**:* gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua un trattamento di dati;

Struttura del Sistema Informativo Aziendale: struttura responsabile dell'ICT (*Information and Communications Technology*) aziendale denominata SOC Tecnologie Informatiche;

Struttura della Gestione delle Risorse Umane: struttura responsabile delle politiche del personale denominata SOC Gestione Risorse Umane.

system tray: identifica quell'area del *desktop* dove vengono visualizzate le icone dei programmi in quel momento in ascolto oppure che stanno eseguendo particolari operazioni (es. una scansione);

switch: rappresenta un dispositivo di rete, solitamente alloggiato in un armadio di rete, che funge da nodo di smistamento dati di una rete di comunicazione;

tablet: *Computer* portatile di dimensioni ridotte, sul cui schermo è possibile scrivere o impartire comandi col tocco delle dita o mediante un apposito stilo;

***Titolare del trattamento**:* la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui compete, anche unitamente ad altro titolare, la decisione in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

***username**:* il nome (identificativo) con il quale l'Utente è riconosciuto da un Computer, da un programma o da un *server*;

***utente**:* ciascuna persona che acceda alle risorse informatiche aziendali;

***web**:* l'abbreviazione di *World Wide Web*, è un servizio *Internet* che permette di navigare ed usufruire di un insieme vastissimo di contenuti collegati tra loro attraverso collegamenti ipertestuali (*link*);

***web filtering**:* è un sistema in grado, di analizzare il contenuto dei siti *web* durante la navigazione e sulla base di criteri prefissati, ad esempio l'origine o la classificazione del contenuto (pubblicità, pornografia, *malware*, virus, ecc…) che consente di filtrare/bloccare la navigazione.

6. Acronimi

***BIOS**: Basic Input-Output System* è un insieme di routine *software*, che fornisce una serie di funzioni di base per l'accesso all'*hardware* e alle periferiche integrate;

***IP**: Internet Protocol* è un'etichetta numerica che identifica univocamente un dispositivo collegato a una rete informatica (protocollo di comunicazione). Un indirizzo IP assolve due funzioni principali: identificare un dispositivo sulla rete e di conseguenza fornirne il percorso per la sua raggiungibilità da un altro terminale o dispositivo di rete. Può essere statico o dinamico;

***LAN**: Local Area Network*: è un gruppo di Computer connessi in un'area locale per comunicare tra loro e condividere risorse quali le stampanti, ecc.;

***PEO**:* Posta Elettronica Ordinaria. La PEO può essere *"ad personam",* oppure associata a specifici funzione/progetto, ufficio o servizio;

***PEC**:* Posta Elettronica Certificata;

SGSI: Sistema di Gestione della Sicurezza delle Informazioni;

***SIIR**:* Sistema Informativo Integrato Regionale è il complesso dell'infrastruttura telematica e delle procedure applicative condivise con tutte le aziende sanitarie della Regione Friuli Venezia Giulia;

UE: Unione Europea

USB: *Universal Serial Bus* indicata con il simbolo , in elettronica, è un'interfaccia per la comunicazione seriale fra dispositivi elettronici. Può essere anche utilizzata per la ricarica della batteria. Esistono diversi tipi di connettore USB: Mini USB, Micro USB, USB Type-C, ecc.;

***VPN**: Virtual Private Network* è una rete privata accessibile solo ad utenti autorizzati creata sfruttando il canale di comunicazione Internet, che permette a dispositivi ubicati in sedi fisiche diverse di stabilire un collegamento sicuro.

7. Riferimenti normativi e bibliografici

- Circolare Agenzia per l'Italia Digitale del 18 aprile 2017 n° 2 "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (DPCM 1° agosto 2015)».GU n.103 del 05 maggio 2017.
- Regolamento Generale sulla Protezione dei Dati UE n. 2016/679;
- Decreto Legislativo del 14 settembre 2015, n. 151" Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183".
- Decreto del Presidente della Repubblica del 16 aprile 2013 n.62 "Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165".
- Legge del 04 aprile 2012 n.35 "Conversione in legge, con modificazioni, del decreto legge 9 febbraio 2012, n. 5, recante disposizioni urgenti in materia di semplificazione e di sviluppo".
- Provvedimento del Garante per la protezione dei dati: "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009" G.U. n. 149 del 30 giugno 2009.
- Provvedimento del Garante per la protezione dei dati: "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" - G.U. n. 300 del 24 dicembre 2008.
- Linee Guida del Garante per la protezione dei dati: "Lavoro: le linee guida del Garante per posta elettronica e Internet" - G.U. n. 58 del 10 marzo 2007.
- Decreto Legislativo del 7 marzo 2005 n. 82 "Codice dell'Amministrazione Digitale" e s.m.i..
- Decreto Legislativo del 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e s.m.i..
- Decreto Legislativo del 8 giugno 2001 n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300".
- Legge del 18 agosto 2000 n. 248 "Nuove norme di tutela del diritto d'autore".
- Decreto Legislativo del 29 dicembre 1992 n.518 "Attuazione della Direttiva n. 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore".
- Legge del 20 maggio 1970 n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento".

8. Documenti interni collegati

Non sono presenti documenti interni collegati.

9. Allegati

Non sono presenti allegati.

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: FRANCESCO MAGRIS
CODICE FISCALE: MGRFNC69D27G888F
DATA FIRMA: 29/04/2022 15:14:11
IMPRONTA: 12B51E580EA6DFDECF2A290361DA9258EBD644B8D21AA1EBC62168AE15589539
EBD644B8D21AA1EBC62168AE15589539E24A825EDFB0AEC941CBFCD36C36C7F0
E24A825EDFB0AEC941CBFCD36C36C7F0E3F1290D2AB03EA3F84BF72659370F8A
E3F1290D2AB03EA3F84BF72659370F8A061E5EF7805205FC48FBD34B9C2B926A

NOME: DAVID TURELLO
CODICE FISCALE: TRLDVD77S13G284T
DATA FIRMA: 29/04/2022 15:29:43
IMPRONTA: 5CC51313DE84CD05E60E800159BCD0C4CEBBF5AC7B3BA12C03EEF76E5262ED35
CEBBF5AC7B3BA12C03EEF76E5262ED35C337501E025124F06B9756CB84091688
C337501E025124F06B9756CB84091688C55AB77E1731A6062D1EF0BBC944B332
C55AB77E1731A6062D1EF0BBC944B3328272644EF7D0300B553245822BC04E19

NOME: DENIS CAPORALE
CODICE FISCALE: CPRDNS75M11C758X
DATA FIRMA: 29/04/2022 15:48:09
IMPRONTA: 7E0BFBD7B56BD435FC802D21D1A33AFAD4459B29AF0BAC213EC2C1549C830CB2
D4459B29AF0BAC213EC2C1549C830CB2028BC3DBA3C0BF492D7B2B28D5147190
028BC3DBA3C0BF492D7B2B28D5147190AE630827C5BAEA2A4C04FCCD255EC338
AE630827C5BAEA2A4C04FCCD255EC338EEE0F94DA7244A7A90A708FB0EC92650