Sanitaservice
ASL TA s.r.l. Unipersonale

ASL Taranto
PugliaSalute

REGOLAMENTO E MISURE DI SICUREZZA AZIENDALI

Responsabile Transizione Digitale
Claudio Fuggetti
Project Manager

Ver. 1.0 del 21/09/2022

GENERALITA'

Il presente documento integra tutte le regole e le disposizioni in materia di sicurezza informatica aziendale partendo dagli aspetti hardware sino agli adeguamenti in materia di trattamento dei dati. La Sanitaservice Asl Ta S.r.l., essendo una società a partecipazione dell'Asl Taranto e prestando i propri servizi all'interno delle strutture della Stessa, utilizza la stessa infrastruttura tecnologica e di telecomunicazione pertanto molte disposizioni sono vincolate a quelle adottate dall'Asl Taranto.

RIFERIMENTI NORMATIVI

- Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", come modificato ed integrato dal D.Lgs.101/2018;
- Provvedimento del Garante per la protezione dei dati personali "Linee guida per posta elettronica e internet" del 01.03.2007"(Gazzetta Ufficiale n. 58 del 10 marzo 2007);
- Provvedimento del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008);
- Provvedimento del Garante "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" del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009);
- Provvedimento del Garante "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali "del 13 ottobre 2008 (Gazzetta Ufficiale n. 287 del 9 dicembre 2008);
- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro";

OGGETTO E FINALITA'

Il presente Regolamento ha per oggetto le politiche di sicurezza dettate per un utilizzo corretto del sistema informativo da parte dell'Utente ed è pertanto finalizzato a:

- garantire la sicurezza, l'integrità, la disponibilità e la riservatezza del sistema informativo;
- tutelare i beni aziendali (beni e risorse informatiche, servizi ICT e reti informatiche);
- assicurare la mitigazione del rischio di data breach (violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati), per prevenire ed evitare condotte inconsapevoli, scorrette o illecite da parte degli Utenti che potrebbero esporre l'Azienda a sanzioni amministrative, danni patrimoniali e di immagine.

SOMMARIO

GENERALITA' 2
RIFERIMENTI NORMATIVI 2
OGGETTO E FINALITA' 3
1. STRUMENTI DI LAVORO ED ASSET CHE IMPATTANO SULLA DATA PROTECTION 6
1.1. Inventario degli asset 6
1.2. Regole utilizzo strumenti aziendali 6
1.3. Gestione dei supporti rimovibili 8
1.4. Adozione di crittografia sulle trasmissioni e sui dati 8
2. GESTIONE DELLA POSTA ELETTRONICA 9
2.1. UTENTI DEL SERVIZIO DI POSTA ELETTRONICA, ACCOUNT ED INDIRIZZI 9
2.2. OBBLIGHI E DIRITTI DELL' AZIENDA 10
2.3. LIMITI DI RESPONSABILITÀ DELL'AZIENDA 10
2.4. RISERVATEZZA POSTA ELETTRONICA 10
2.5. DOVERI, DIVIETI, LIMITI DI UTILIZZO, RESPONSABILITÀ DELL'UTENTE 11
2.6. LISTE DI DISTRIBUZIONE 12
2.7. REVOCA DEL SERVIZIO 12
3. GESTIONE DEGLI APPLICATIVI AZIENDALI 14
4. SMARTWORKING 15
5. ASSISTENZA TECNICA 18
6. CONTROLLO PROFONDITÀ E REQUISITI DEGLI ACCESSI 19
6.1. Definizione preventiva dei requisiti e configurazione degli accessi consentiti e dei permessi dei singoli soggetti autorizzati 19
6.2. Controllo e politiche di accesso alle reti ed ai servizi di rete 19
6.3. Registrazione e de-registrazione degli utenti 20
6.4. Gestione dei diritti di accesso privilegiato (Ads) 21
6.5. Gestione delle informazioni segrete di autenticazione degli utenti 21
7. SICUREZZA FISICA ED AMBIENTALE 22
7.1. Gestione di specifiche Aree ove necessitano più elevati standard di sicurezza 22
7.2. Adozione di misure per la sicurezza fisica del perimetro 22
7.3. Controlli per l'accesso fisico alle sedi ove sono conservati i dati 22
7.4. Sicurezza fisica 22
8. SICUREZZA DELLE ATTIVITÀ OPERATIVE 23
8.1. Protezione e controlli contro malware virus attacchi informatici 23

8.2. Aggiornamento software, applicativi e manutenzione generale del sistema informativo scadenzata e comprovabile 23
8.3. Backup delle informazioni 23
8.4. Prove di ripristino dei dati 24
8.5. Raccolta di log e monitoraggio di sicurezza 24
8.6. Protezione delle informazioni di log 25
8.7. Log di amministratori e operatori 25
8.8. controlli su Installazione ed uso software o strumenti non autorizzati 25
DI SISTEMA 25
9. SICUREZZA DELLE COMUNICAZIONI 26
9.1. Sicurezza dei servizi di rete 26
9.2. Politiche e procedure per il trasferimento delle informazioni 26
9.3. Gestione dell'erogazione dei servizi dei fornitori, tramite valutazione degli stessi accordi contrattuali scritti, verifica del loro operato 26
10. GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI 27
10.1. Gestione degli incidenti relativi alla sicurezza dei dati 27
10.2. Definizione Responsabilità e procedure 27
10.3. Segnalazione degli eventi relativi alla sicurezza 27
10.4. Procedure di segnalazione dei Breach 27
10.5. Raccolta di evidenze e registro incidenti 28
11. DISASTER RECOVERY E CONTINUITÀ OPERATIVA 28
11.1. Attuazione di processi di disaster recovery 28
11.2. Attuazione processi di continuità operativa 28

1. STRUMENTI DI LAVORO ED ASSET CHE IMPATTANO SULLA DATA PROTECTION

1.1. INVENTARIO DEGLI ASSET

E' necessario specificare che esistono beni di proprietà della Società e beni di proprietà dell'Asl Taranto (hub, router, swith di rete, firewall, ecc); questi ultimi seguiranno le regole e disposizioni generali dell'Asl Taranto.

Gli asset relativi alla dotazione informatica aziendale sono ineriti in un registro elettronico, di competenza dell'ufficio del Responsabile della Transizione digitale conservato presso gli archivi digitali e denominato "Inventario dotazione informatica", ed etichettati dall''ufficio del Patrimonio subito dopo aver completato le attività di acquisto.

1.2. REGOLE UTILIZZO STRUMENTI AZIENDALI

Gli strumenti informatici sono il complesso di dispositivi fisici (PC, stampanti, lettori portatili, smartphone, ed altri devices) messi a disposizione dell'Utente per il perseguimento degli obiettivi aziendali.

Ogni Utente è responsabile dell'integrità e della custodia dei dispositivi fisici e delle informazioni/dati allo stesso affidati dall'Azienda.

Ad ogni dispositivo è associato un numero di inventario, la collocazione fisica e l'Utente, allo scopo di curare il parco dispositivi aziendale e definire le responsabilità in caso di furto, smarrimento o guasto volontario.

Qualsiasi spostamento permanente del dispositivo (es. trasloco, assegnazione ad altro reparto, assegnazione ad altro professionista) deve essere concordata l'Area del Patrimonio e con l'Amministratore di sistema allo scopo di consentirne la tracciabilità.

Qualora occorra, i dispositivi possono anche essere utilizzati in condivisione con qualsiasi operatore dell'Azienda, con la previsione della sessione individuale di lavoro per ogni utente e specifiche credenziali di identificazione ed autenticazione relative al dominio dell'Asl Taranto.

Il Personal Computer è fornito all'Utente con una configurazione software predefinita che non può essere dallo stesso modificata autonomamente. La configurazione dei profili abilitativi di tutti gli utenti aziendali è eseguita con

privilegi che non consentono l'installazione o l'esecuzione di programmi non autorizzati sulle macchine client e sui server.

Nell'uso dei dispositivi informatici, quali strumenti di lavoro, l'Utente è tenuto alle seguenti prescrizioni di carattere generale:

- utilizzare i dispositivi fisici con consapevolezza, appropriatezza e professionalità unicamente per finalità compatibili con le attività aziendali;
- custodire con cura e diligenza i dispositivi fisici per evitare la sottrazione, la distruzione o il danneggiamento;
- è fatto assoluto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi, di rimuovere, danneggiare o asportare componenti hardware, ovvero di modificare la configurazione hardware e software del proprio dispositivo;
- non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche.
- è vietato collegare alla rete aziendale Personal Computer, PC portatili ed altri dispositivi hardware che non appartengano all'Azienda, senza l'autorizzazione dell'Azienda stessa, dell'Amministratore di sistema; è vietato l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall' Amministratore di sistema o dal Referente Informatico; l'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre a gravi responsabilità civili, oltre che penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.
- non lasciare incustodita la postazione di lavoro con la sessione utente attiva;
- in caso di allontanamento dalla propria postazione di lavoro, spegnere il PC o bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password, ovvero disconnettersi, effettuando il log-out dalla sessione;
- al termine del lavoro spegnere il proprio dispositivo;
- eseguire il backup periodico (almeno settimanale) dei dati secondo le indicazioni dell'Amministratore di sistema (ad es. su NAS o su supporto magnetico per i trattamenti di dati non gestiti dalla Rete Informatica aziendale, ecc.); nel caso di salvataggio su supporto magnetico rimovibile l'Utente deve sostituire periodicamente tali supporti e provvedere alla loro conservazione in un luogo sicuro;
- non caricare o inserire all'interno del dispositivo fisso o portatile dati personali non attinenti con l'attività lavorativa svolta; in ogni caso, prima della riconsegna di tali dispositivi per restituzione o riparazione, gli Utenti sono obbligati a cancellare tutti i dati personali eventualmente presenti.

1.3. GESTIONE DEI SUPPORTI RIMOVIBILI

I supporti rimovibili sono quei dispositivi che consentono di copiare o archiviare dati, files o documenti esternamente al computer (CD-ROM, DVD, penne o chiavette USB, hard disk portatili, ecc.).

- L'uso di supporti di memorizzazione rimovibili è in via generale sconsigliabile.
- Qualora il loro utilizzo si renda assolutamente necessario, l'Utente è tenuto ad adottare le seguenti cautele:
  - utilizzare i dispositivi rimovibili aziendali esclusivamente su computer aziendali;
  - prima dell'uso, sottoporre sempre tutti i supporti di origine esterna a scansione antivirus/antimalware con un programma antivirale aggiornato ed avvertire immediatamente l'Amministratore di sistema del rilevamento di virus o malware di qualsiasi natura;
  - qualora vi sia la assoluta necessità di memorizzare su dispositivi rimovibili dati particolari, l'Utente è tenuto ad adottare sistemi di crittografia, avendo cura di permettere la lettura solo agli aventi diritto, ovvero, in mancanza, utilizzare sistemi di pseudonimizzazione (ad esempio, contrassegnando i documenti semplicemente con un codice) o sistemi di anonimizzazione;
  - custodire con cura i supporti rimovibili su cui sono memorizzati dati personali in armadi chiusi a chiave, al fine di evitare che il contenuto possa essere trafugato, o alterato, e/o distrutto, ovvero conosciuto da terzi non autorizzati ad accedervi;
  - procedere alla cancellazione "sicura" dei dati personali presenti sui supporti magnetici od ottici, prima del loro riutilizzo;
  - consegnare i supporti magnetici obsoleti (dischetti, nastri, chiavi USB, CD riscrivibili ed altro) all'Amministratore di sistema per l'opportuna distruzione, onde evitare che il loro contenuto possa essere recuperato successivamente alla cancellazione.

1.4. ADOZIONE DI CRITTOGRAFIA SULLE TRASMISSIONI E SUI DATI

I dati vengono attraverso la rete intranet, il cui proprietario è l'Asl Taranto, ttraverso il protocollo TCP.

Mentre per quanto riguarda il trasferimento dei dati attraverso mail, pec o portali dei fornitori o bancari è utilizzato lo standard di crittografia TLS.

2. GESTIONE DELLA POSTA ELETTRONICA

Il servizio di Posta elettronica è fornito dall'Azienda in funzione della comunicazione, della amministrazione e delle altre attività strumentali correlate ai fini istituzionali. Il servizio è subordinato all'osservanza integrale delle condizioni di seguito indicate. L'utilizzo del servizio da parte dell'Utente costituisce implicita accettazione delle citate condizioni.

La casella di posta assegnata all'Utente è uno strumento di lavoro messo a disposizione per lo svolgimento della prestazione lavorativa. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2.1. UTENTI DEL SERVIZIO DI POSTA ELETTRONICA, ACCOUNT ED INDIRIZZI

L'account di posta elettronica (username, password ed indirizzo di posta) è fornito, insieme ad un limitato spazio disco, alle seguenti categorie di Utenti:

- Organi, Strutture ed articolazioni aziendali centrali e periferiche Aree di gestione, Uffici di Staff; in questo caso il formato dell'indirizzo di posta sarà: nomeservizio@sanitaserviziaslta.it.
- Personale dipendente in servizio attivo; in questo caso il formato dell'indirizzo di posta sarà: nome.cognome@ sanitaserviziaslta.it. con eccezioni previste per casi di omonimia.

L'attivazione dell'account avverrà, a cura dell'amministratore del sistema che ha diritti e privilegi di Postmaster, su richiesta scritta autorizzata dal Dirigente responsabile del Settore e/o dal dipendente e/o dell'Ufficio del Personale, dopo la verifica dei requisiti richiesti a cura dell'Ufficio del Responsabile della Transizione Digitale.

L'Utente si impegna ad adoperarsi attivamente per salvaguardare la riservatezza della sua password ed a segnalare qualunque situazione che possa inficiarla.

L'Utente sarà responsabile dell'attività espletata tramite il suo account.

La "personalizzazione" dell'indirizzo non comporta il suo carattere "privato", in quanto trattasi di strumenti di esclusiva proprietà aziendale messi a disposizione dell'Utente al solo fine dello svolgimento delle proprie mansioni lavorative.

2.2. OBBLIGHI E DIRITTI DELL' AZIENDA

L'Azienda si impegna ad utilizzare i dati forniti dall'Utente ai fini dell'erogazione e gestione del servizio e di attuare quanto in suo potere per proteggere la privacy dell'Utente medesimo.

L'Azienda si impegna a fornire il servizio in modo continuativo, fatte salve eventuali sospensioni dovute all'ordinaria o straordinaria manutenzione, a malfunzionamenti e ad altre eventualità.

Inoltre, l'Azienda si impegna ad effettuare regolari backup generali sui server gestiti direttamente; non sono previsti backup e ripristini individuali.

Tutte le informazioni eventualmente raccolte saranno utilizzate a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento Aziendale, che costituisce adeguata informazione sul trattamento dei dati, sulle modalità d'uso degli strumenti e sull'effettuazione dei controlli ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300.

2.3. LIMITI DI RESPONSABILITÀ DELL'AZIENDA

L'Azienda attuerà tutte le misure ritenute necessarie e sufficienti a minimizzare il rischio di perdita d'informazioni; ciò nonostante l'Utente solleva l'Azienda da ogni responsabilità ed obbligazione in relazione alla cancellazione, al danneggiamento, al mancato invio/ricezione o all'omessa conservazione di messaggi di posta (e-mail) imputabili ad un uso inappropriato del servizio, mentre le responsabilità derivanti da guasti e/o malfunzionamenti degli apparati di gestione del software sono regolate dal contratto di affidamento Servizio come per Legge.

2.4. RISERVATEZZA POSTA ELETTRONICA

L'Azienda persegue la riservatezza e l'integrità dei messaggi durante il loro transito e la loro permanenza nel sistema di posta.

Per il raggiungimento di tale obiettivo il Postmaster si avvarrà anche di strumenti idonei a verificare, mettere in quarantena o cancellare i messaggi che potrebbero compromettere il buon funzionamento del servizio.

Salvo quanto previsto al precedente capoverso i messaggi di posta sono conservati nella mailbox associata all'Utente, finché non vengano dallo stesso rimossi.

2.5. DOVERI, DIVIETI, LIMITI DI UTILIZZO, RESPONSABILITÀ DELL'UTENTE

L'Utente si impegna, nei confronti dell'Azienda, a presidiare quotidianamente la propria casella elettronica, con l'apertura e lettura dei messaggi di posta, corrispondendo alla richiesta di avviso di recapito e monitorando costantemente le sue dimensioni per non superare il limite di spazio previsto.

L'Utente si impegna a non utilizzare il servizio per scopi illegali o non conformi al presente regolamento o che comunque possano recar danno o pregiudizio all'Azienda medesima o a terzi.

L'Utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio; esonera contestualmente l'Azienda da ogni pretesa o azione che dovesse essere rivolta all'Azienda medesima da qualunque soggetto, in conseguenza di tale uso improprio del servizio.

L'Utente, inoltre, non può utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con l'utilizzo da parte di altri utenti.

L'Utente, salvo giustificabili eccezioni, di cui comunque risponde personalmente, non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino a:

- pubblicità non istituzionale, manifesta o occulta;
- comunicazioni commerciali private;
- materiale pornografico o simile, in particolare in violazione della Legge n. 269 del 1998 "Norme contro lo sfruttamento sessuale dei minori degli anni 18";
- materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
- materiale che violi la normativa vigente sulla protezione dei dati personali;
- contenuti o materiali che violino i diritti di proprietà di terzi;
- altri contenuti illegali.

In nessun caso l'Utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili.

L'Utente non può tentare di accedere, in modo non autorizzato, ad altri account, a sistemi o ad altre reti tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti.

L'utente si impegna a fare attenzione alle mail ingannevoli, controllando i file allegati di posta elettronica prima del loro utilizzo; deve evitare di aprire gli allegati e di cliccare i link contenuti in messaggi di mittenti sconosciuti, notificando l'accaduto all'Amministratore di sistema o al Referente informatico e cancellando tali mail.

Per l'invio a destinatari esterni di messaggi contenenti allegati relativi a dati personali particolari o giudiziari, l'Utente è tenuto a renderli preventivamente illeggibili, criptandoli con apposito software e comunicando al destinatario la password di cifratura attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono).

L'Utente, infine, si impegna a non divulgare messaggi di natura ripetitiva (catene di varia denominazione) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

Di fronte a quest'ultima evenienza l'Utente dovrà limitarsi ad inoltrare un messaggio al Postmaster@sanitaserviceaslta.it.

L'Utente accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e assume l'onere di comunicare, tempestivamente, all'Amministratore di sistema, la ricezione di posta "indesiderata" per le opportune protezioni.

2.6. LISTE DI DISTRIBUZIONE

Allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali, è previsto l'uso delle liste di distribuzione (mailing list), personali o centralizzate. L'utente può avvalersi di liste di distribuzione personali, per le proprie necessità funzionali, salvo limitazioni operate dal Postmaster, a fronte di esigenze tecniche e/o gestionali.

Una lista generale di distribuzione, centralizzata e comprendente tutti gli utenti, è gestita dal Postmaster.

Oltre alla lista generale di distribuzione, sono possibili altre liste centralizzate (o gruppi) utili a soddisfare le esigenze di categorie omogenee di utenti; l'attivazione di questi gruppi è a cura del Postmaster che valuterà, di volta in volta, le specifiche richieste.

2.7. REVOCA DEL SERVIZIO

L'Utente riconosce e concorda che l'Azienda può revocargli l'account, ovvero sospenderne temporaneamente l'utilizzo, in caso di violazione del presente regolamento.

Inoltre, l'Azienda si riserva il diritto di interrompere o sospendere, in tutto o in parte, l'erogazione del Servizio per motivi tecnici o amministrativi.

In caso di interruzione del rapporto di lavoro a qualsiasi titolo, l'indirizzo di posta elettronica dell'Utente sarà disabilitato.

3. GESTIONE DEGLI APPLICATIVI AZIENDALI

Gli applicativi aziendali sono l'insieme dei programmi (software) che consentono l'inserimento, l'archiviazione, l'elaborazione e la consultazione dei dati aziendali, sfruttando i dispositivi hardware e le connessioni di rete dell'Azienda.

Essi devono rispondere ai requisiti di confidenzialità, integrità, continuità del dato e riconducibilità al singolo Utente, come prescritto dal Regolamento Europeo 2016/679 per il trattamento dei dati personali.

Gli Utenti e gli Amministratori di sistema devono possedere le sole autorizzazioni strettamente necessarie ad effettuare il loro compito. In ogni caso, ciascuno deve astenersi da effettuare operazioni che, ancorché tecnicamente consentite dai sistemi, non rientrano nella propria mansione specifica.

Pertanto, gli applicativi software devono prevedere profili di autorizzazione di ambito diverso per diversi incaricati, in modo da consentire che solo alcuni di essi possano effettuare alcuni trattamenti o accedere a certi tipi di dato.

L'abilitazione dell'Utente agli applicativi aziendali avviene su esplicita richiesta avanzata dal Responsabile della Struttura all'Amministratore di sistema.

Periodicamente, con cadenza almeno annuale, sono aggiornati gli ambiti del trattamento consentito agli addetti, a cura dell'Amministratore di sistema con il supporto dei responsabili delle UU.OO.CC..

Per un corretto utilizzo degli applicativi aziendali l'Utente deve:

- garantire la correttezza del dato, prevenendo il rischio di trattamenti impropri (inserimento di dati non corretti, mancato inserimento di dati, accesso a dati non pertinenti, ecc.);
- non utilizzare account assegnati ad altri Utenti;
- non comunicare ad altri le proprie credenziali personali di autenticazione, anche se solo temporaneamente;
- effettuare la pronta segnalazione di qualsiasi malfunzionamento.

4. SMARTWORKING

L'Azienda può mettere a disposizione degli Utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna.

Anche in tal caso l'Utente (ad es. smart-worker) è tenuto a conformarsi a tutte le prescrizioni di sicurezza dettate nel presente Regolamento, per quanto compatibili. Inoltre, l'Utente abilitato ad accedere alle risorse informatiche aziendali dall'esterno è tenuto a:

- individuare uno spazio idoneo per predisporre la propria postazione lavorativa da utilizzare in modo esclusivo, ponendo ogni cura per evitare che ai dati possano accedere persone non autorizzate;
- assicurarsi della conformità delle prese elettriche prima di utilizzarle per alimentare il dispositivo o i dispositivi aziendali;
- assicurarsi che la postazione scelta non possa essere investita da acqua, fuoco, vento, calore eccessivo;
- non lasciare incustodita la postazione di lavoro e riporre gli strumenti di lavoro in armadietti chiusi a chiave al termine di ogni sessione lavorativa; usare meccanismi (cifratura dei dati, pasword di sicurezza, ecc.) che consentano di inibire la possibilità di accesso ai dati a chi dovesse entrarne in possesso;
- bloccare l'elaboratore in dotazione in caso di allontanamento dalla propria postazione di lavoro, anche per un intervallo molto limitato;
- adoperare "misure di sicurezza" nell'utilizzo di pc o tablet come para schermi (privacy- screen) che impediscano la visuale laterale al vicino;
- non condividere con i colleghi documenti aziendali o attività lavorative su piattaforme come Google document, ovvero altre simili e/o comunque piattaforme diverse da quella aziendale o da quella indicata dal datore di lavoro;
- utilizzare il dispositivo aziendale solo ed esclusivamente per le attività lavorative;
- a conclusione della prestazione lavorativa giornaliera conservare e tutelare i documenti eventualmente stampati, provvedendo alla loro eventuale distruzione con particolare accuratezza, utilizzando appositi

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceasl ta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
sanitaservice@asl.taranto.it
Sede Legale: Viale Virgilio, 31 – 74123 Taranto
0994585171 Uff. Finanziarie
sanitaserviceasl ta@pec.it
Sede Operativa:
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo

apparecchi "distruggi documenti" o, in mancanza, sminuzzandoli in modo da non renderli più ricomponibili.

Qualora l'Utente (smart-worker) sia anche autorizzato all'uso di un dispositivo client remoto proprio, è altresì tenuto ad osservare le seguenti disposizioni per assicurare lo stesso livello di sicurezza dei dispositivi client aziendali:

- utilizzare sui dispositivi client solo sistemi operativi per i quali è garantito l'aggiornamento;
- effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo del dispositivo client utilizzato;
- installare un adeguato sistema antivirus/antimalware da tenere costantemente aggiornato;
- collegarsi a dispositivi mobili (ad es.pen-drive) solo se si conosce la provenienza (ad es. nuovi, forniti dall'Amministrazione) ed, in ogni caso, effettuare una scansione preventiva di tutti i supporti rimovibili utilizzati;
- evitare di utilizzare il dispositivo adoperato per lo smart-working per l'uso di social network o altre applicazioni social facilmente hackerabili;
- verificare che gli accessi al sistema operativo siano protetti da password sicura, conforme alle disposizioni del presente Regolamento;
- non installare sul dispositivo utilizzato software proveniente da fonti/repository non ufficiali;
- utilizzare l'accesso a reti adeguatamente protette;
- non utilizzare pc pubblici o comunque di terzi, né reti Wi-Fi pubbliche, le quali possono essere un veicolo che consente più facilmente di condurre attacchi ai dispositivi;
- effettuare sempre il log-out dai servizi/portali utilizzati dopo che si è conclusa la sessione lavorativa;
- non cliccare su link o allegati contenuti in e-mail sospette;
- utilizzare strumenti di crittografia in caso di condivisione di dati particolari per posta elettronica.

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
31 – 74123 Taranto
0994585171 Uff. Finanziarie
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo
sanitaservice@asl.taranto.it
sanitaserviceaslta@pec.it
Sede Legale: Viale Virgilio,
Sede Operativa:

Si precisa che le forme di accesso consentite tra il dispositivo dell'Utente ed il server aziendale sono solo le connessioni sicure (ad es. VPN – Virtual Private Network).

Esse comportano la registrazione degli accessi in file Log (ad es. nome utente, indirizzo IP di provenienza, orari in cui tali operazioni vengono effettuate) per finalità di tutela della sicurezza, riservatezza ed integrità dei dati aziendali trattati.

L'Amministratore di Sistema è tenuto al controllo della sicurezza delle postazioni esterne remote, negando o interrompendo l'accesso alla rete agli Utenti che utilizzino dispositivi non adeguatamente protetti e/o aggiornati che possano costituire una concreta minaccia per la sicurezza informatica dell'Azienda.

Il presente Regolamento Aziendale costituisce adeguata informazione sul trattamento dei dati personali, sulle modalità d'uso delle risorse informatiche e sull'effettuazione dei controlli, ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300.

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
31 – 74123 Taranto
0994585171 Uff. Finanziarie
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo
sanitaservice@asl.taranto.it
sanitaserviceaslta@pec.it
Sede Legale: Viale Virgilio,
Sede Operativa:

5. ASSISTENZA TECNICA

Le attività di manutenzione, gestione ed implementazione sono eseguite da personale interno nominato dal Titolare quale autorizzato al trattamento ai sensi dell'art. 29 GDPR, a cui sono impartite apposite istruzioni, ovvero da singoli professionisti e/o da personale afferente all'organizzazione di soggetti esterni nominati dal Titolare quali responsabili del trattamento ai sensi dell'art. 28 GDPR.

Tali soggetti esterni, a cui sono impartiti specifici obblighi di riservatezza, devono essere in grado di fornire garanzie adeguate al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

A seguito di chiamata dell'Utente o in caso di necessità per la rilevazione tecnica di problemi nel sistema informatico, l'Amministratore di sistema ed il suddetto personale incaricato del servizio sono autorizzati a compiere interventi nel sistema informatico aziendale per risolvere problemi tecnici e/o manutentivi, nonché per garantire la sicurezza e la salvaguardia del sistema.

Per le suddette finalità, gli interventi tecnici potranno anche comportare l'accesso ai dati trattati da ciascun Utente, ivi compreso l'accesso agli archivi di posta elettronica e la verifica dei siti internet a cui hanno avuto accesso gli Utenti abilitati alla navigazione esterna.

Il suddetto personale potrà collegarsi e visualizzare in remoto il desktop delle singole postazioni, dandone preventiva comunicazione all'interessato, qualora non si pregiudichi la necessaria tempestività e l'efficacia dell'intervento tecnico.

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
31 – 74123 Taranto
0994585171 Uff. Finanziarie
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo
sanitaservice@asl.taranto.it
sanitaserviceaslta@pec.it
Sede Legale: Viale Virgilio,
Sede Operativa:

6. CONTROLLO PROFONDITÀ E REQUISITI DEGLI ACCESSI

6.1. DEFINIZIONE PREVENTIVA DEI REQUISITI E CONFIGURAZIONE DEGLI ACCESSI CONSENTITI E DEI PERMESSI DEI SINGOLI SOGGETTI AUTORIZZATI

6.2. CONTROLLO E POLITICHE DI ACCESSO ALLE RETI ED AI SERVIZI DI RETE

L'articolo 23 del recente D.lgs. 14 settembre 2015 n. 151 ("Jobs Act") ha modificato il contenuto dell'articolo 4 della Legge 300/1970, ora rubricato "Impianti audiovisivi e altri strumenti di controllo".

Alla luce delle suddette disposizioni, l'Azienda può effettuare controlli sugli strumenti informatici utilizzati dal lavoratore per rendere la prestazione lavorativa (personal computer, tablet, telefoni e smartphone), senza la necessità di accordi sindacali preventivi, fornendo al lavoratore un'adeguata informativa sulle regole previste per l'utilizzo lavorativo ed eventualmente personale degli strumenti di cui si tratta e sulle modalità e i casi in cui potranno essere effettuati i controlli.

Per quanto innanzi l'Azienda, in qualità di datore di lavoro, si riserva la facoltà di effettuare controlli, anche saltuari o occasionali, sui dispositivi utilizzati dall'Utente per rendere la prestazione lavorativa (computer, tablet, ecc.).

Gli eventuali controlli saranno eseguiti in conformità della normativa vigente, con particolare riferimento al Regolamento Europeo 2016/679, al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, all'articolo 4 comma 2 della della Legge 300/1970, come modificato dal D.Lgs. 14/09/2015 n°151 ed ai provvedimenti emanati dal Garante.

A tale scopo, con il presente Regolamento aziendale, all'Utente è fornita adeguata informazione in ordine alla modalità d'uso degli strumenti e di effettuazione dei controlli, nonché informativa sul trattamento dei dati

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
sanitaservice@asl.taranto.it
Sede Legale: Viale Virgilio, 31 – 74123 Taranto
0994585171 Uff. Finanziarie
sanitaserviceaslta@pec.it
Sede Operativa:
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo

personali ai sensi dell'art. 13 del Regolamento UE 2016/679 (vedi successivo art. 15).

I controlli sull'uso degli strumenti elettronici saranno tali da evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori e di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

Gli eventuali controlli saranno commisurati allo scopo e saranno effettuati nel rispetto dei principi di necessità, pertinenza e non eccedenza, proporzionalità e gradualità.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, l'Azienda può adottare eventuali misure che consentano la verifica di comportamenti anomali.

In tal caso, il personale incaricato effettuerà per quanto possibile un controllo preliminare su dati aggregati, riferiti all´intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l´invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.

L´avviso può essere circoscritto anche a dipendenti afferenti all´area o settore in cui è stata rilevata l´anomalia.

Sono, comunque, esclusi controlli prolungati, costanti o indiscriminati.

In caso di reiterate anomalie o irregolarità, ovvero di segnalazioni di attività non conformi alla normativa vigente ed al presente Regolamento, saranno effettuati controlli su base individuale.

6.3. REGISTRAZIONE E DE-REGISTRAZIONE DEGLI UTENTI

Gli utenti saranno inseriti nel sistema informativo con i relativi permessi solo dopo apposita richiesta formulata all'Amministratore di sistema attraverso modulo inoltrato via mail all'indirizzo rtd@sanitaserviceaslta.it . In caso di spostamento o dimissioni del dipendente le sue credenziali saranno sospese previa comunicazione da parte dell'Ufficio del Personale.

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
sanitaservice@asl.taranto.it
Sede Legale: Viale Virgilio, 31 – 74123 Taranto
0994585171 Uff. Finanziarie
sanitaserviceaslta@pec.it
Sede Operativa:
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo

6.4. GESTIONE DEI DIRITTI DI ACCESSO PRIVILEGIATO (ADS)

L'unico utente con diritti di accesso privilegiato è l'Amministratore di sistema.

6.5. GESTIONE DELLE INFORMAZIONI SEGRETE DI AUTENTICAZIONE DEGLI UTENTI

L' Azienda, nel rispetto della normativa vigente sulla protezione dei dati, si riserva il diritto di accedere alla risorsa informatica in dotazione dell'Utente ed ai documenti in essa contenuti, per esigenze organizzative e produttive (attività di gestione, controllo, aggiornamenti ai fini della sicurezza del sistema e della rete), per la sicurezza del lavoro e per la tutela del patrimonio, nella considerazione che ogni dato trattato per mezzo degli strumenti e delle risorse informatiche appartenenti all'Azienda sarà considerato di natura aziendale e non riservata.

I log relativi all'utilizzo degli strumenti, reperibili nella memoria degli strumenti, ovvero sui server o sui router, ivi compresi i file log riferiti al traffico web ed alla connessione VPN, sono registrati e possono essere oggetto di controllo attraverso l'Amministratore di sistema.

Le informazioni raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento.

Il presente Regolamento Aziendale costituisce adeguata informazione in ordine al trattamento dei dati personali, alla modalità d'uso degli strumenti e di effettuazione dei controlli, ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300.

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
31 – 74123 Taranto
0994585171 Uff. Finanziarie
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo
sanitaservice@asl.taranto.it
sanitaserviceaslta@pec.it
Sede Legale: Viale Virgilio,
Sede Operativa:

7. SICUREZZA FISICA ED AMBIENTALE

7.1. GESTIONE DI SPECIFICHE AREE OVE NECESSITANO PIÙ ELEVATI STANDARD DI SICUREZZA

La sala CED dove sono ospitati i server aziendali è di proprietà dell'Asl Taranto quindi la gestione della stessa dal punto di vista della manutenzione e degli standard di sicurezza è in carico all'Asl Taranto.

7.2. ADOZIONE DI MISURE PER LA SICUREZZA FISICA DEL PERIMETRO

Come sopra.

7.3. CONTROLLI PER L'ACCESSO FISICO ALLE SEDI OVE SONO CONSERVATI I DATI

Come sopra.

7.4. SICUREZZA FISICA

Come sopra.

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
31 – 74123 Taranto
0994585171 Uff. Finanziarie
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo
sanitaservice@asl.taranto.it
sanitaserviceaslta@pec.it
Sede Legale: Viale Virgilio,
Sede Operativa:

8. SICUREZZA DELLE ATTIVITÀ OPERATIVE

8.1. PROTEZIONE E CONTROLLI CONTRO MALWARE VIRUS ATTACCHI INFORMATICI

Le informazioni e le infrastrutture IT di proprietà dell'Azienda devono essere protette dal malware.

In particolare, i programmi antivirus/antimalware devono essere installati su tutti gli apparati, sia server che postazioni di lavoro e devono essere aggiornati almeno semestralmente.

Per prevenire le vulnerabilità derivanti, l'Utente deve osservare comportamenti idonei a ridurre il rischio di attacco al sistema informatico aziendale.

In particolare, ogni Utente è obbligato a controllare la presenza e il regolare funzionamento del programma antivirus/antimalware aziendale e consentire i periodici aggiornamenti dello stesso. Qualora il programma antivirus/antimalware rilevi la presenza di un malware, l'Utente dovrà sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto all'Amministratore di Sistema.

L'Utente è tenuto, altresì, a verificare mediante il programma antivirus/antimalware ogni dispositivo magnetico di provenienza esterna all'Azienda prima del suo utilizzo.

8.2. AGGIORNAMENTO SOFTWARE, APPLICATIVI E MANUTENZIONE GENERALE DEL SISTEMA INFORMATIVO SCADENZATA E COMPROVABILE

L'aggiornamento dei sistemi operativi seguirà la politica di dominio dell'Asl Taranto. Per quanto riguarda gli applicativi utilizzati nella intranet saranno eseguiti tutti gli aggiornamenti necessari per garantire la sicurezza dei sisitemi.

8.3. BACKUP DELLE INFORMAZIONI

Le copie di backup delle informazioni, del software e delle immagini dei sistemi residenti sui server aziendali o sui NAS devono essere effettuati

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
sanitaservice@asl.taranto.it
Sede Legale: Viale Virgilio, 31 – 74123 Taranto
0994585171 Uff. Finanziarie
sanitaserviceaslta@pec.it
Sede Operativa:
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo

dall'Amministratore di sistema e/o dal personale incaricato all'uopo, con frequenza giornaliera.

A cura dell' Amministratore di sistema è predisposto un piano di verifica periodica del corretto funzionamento delle copie di Backup (le copie sono sottoposte a test periodici di restore).

Per assicurare il ripristino dei dati, le copie di backup della sala server devono essere replicate in un datacenter secondario (disaster recovery).

8.4. PROVE DI RIPRISTINO DEI DATI

A cura dell'Amministratore di sistema sono adottate idonee misure per garantire il ripristino dell'accesso ai dati, in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a 7 giorni.

8.5. RACCOLTA DI LOG E MONITORAGGIO DI SICUREZZA

L' Azienda, nel rispetto della normativa vigente sulla protezione dei dati, si riserva il diritto di accedere alla risorsa informatica in dotazione dell'Utente ed ai documenti in essa contenuti, per esigenze organizzative e produttive (attività di gestione, controllo, aggiornamenti ai fini della sicurezza del sistema e della rete), per la sicurezza del lavoro e per la tutela del patrimonio, nella considerazione che ogni dato trattato per mezzo degli strumenti e delle risorse informatiche appartenenti all'Azienda sarà considerato di natura aziendale e non riservata.

I log relativi all'utilizzo degli strumenti, reperibili nella memoria degli strumenti, ovvero sui server o sui router, ivi compresi i file log riferiti al traffico web ed alla connessione VPN, sono registrati e possono essere oggetto di controllo attraverso l'Amministratore di sistema.

Le informazioni raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento.

Il presente Regolamento Aziendale costituisce adeguata informazione in ordine al trattamento dei dati personali, alla modalità d'uso degli strumenti e di effettuazione dei controlli, ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300.

8.6. PROTEZIONE DELLE INFORMAZIONI DI LOG

I log saranno conservati nell'archivio digitale dell'azienda il cui accesso sarà esclusivamente dell'Amministratore di sistema.

8.7. LOG DI AMMINISTRATORI E OPERATORI

I log saranno conservati nell'archivio digitale dell'azienda il cui accesso sarà esclusivamente dell'Amministratore di sistema.

8.8. CONTROLLI SU INSTALLAZIONE ED USO SOFTWARE O STRUMENTI NON AUTORIZZATI

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
31 – 74123 Taranto
0994585171 Uff. Finanziarie
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo
sanitaservice@asl.taranto.it
sanitaserviceaslta@pec.it
Sede Legale: Viale Virgilio,
Sede Operativa:

9. SICUREZZA DELLE COMUNICAZIONI

9.1. SICUREZZA DEI SERVIZI DI RETE

I servizi di rete sono strettamente dipendenti dalle politiche e dalle regole dell'Asl Taranto essendo l'infrastruttura di proprietà dell'azienda locale.

9.2. POLITICHE E PROCEDURE PER IL TRASFERIMENTO DELLE INFORMAZIONI

Le informazioni potranno essere trasferite solo ed esclusivamente attraverso la posta elettronica aziendale.

9.3. GESTIONE DELL'EROGAZIONE DEI SERVIZI DEI FORNITORI, TRAMITE VALUTAZIONE DEGLI STESSI ACCORDI CONTRATTUALI SCRITTI, VERIFICA DEL LORO OPERATO

L'erogazione di servizi da parte di terzi nel sistema informativo aziendale avviene attraverso standard di sicurezza che prevedono utilizzo di credenziali personali ed identificabili sempre attraverso strumenti di sicurezza adeguati come ad esempio la VPN aziendale.

L'azienda provvederà periodicamente alla verifica del loro operato.

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
31 – 74123 Taranto
0994585171 Uff. Finanziarie
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo
sanitaservice@asl.taranto.it
sanitaserviceaslta@pec.it
Sede Legale: Viale Virgilio,
Sede Operativa:

10. GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI

10.1. GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DEI DATI

In caso di incidenti che compromettono la sicurezza informatica è necessario che venga fatta un'analisi approfondita partendo dagli eventi recenti segnalati.

Nella ricerca dei dati violati devono essere indicati anche i livelli di impatto e i soggetti passivi di tali informazioni- perse/divulgate; a tal proposito i livelli possono essere basso (dati non personali oppure alto dati personali-sanitari).

Identificate le informazioni, le stesse devono essere recuperate attraverso le politiche di back-up oppure rimosse dai connettori di divulgazione e devono essere comunicate al DPO aziendale.

10.2. DEFINIZIONE RESPONSABILITÀ E PROCEDURE

LE responsabilità saranno individuate in base all'ambito di applicazione e al livello di autorizzazione a cui sono sottoposti gli utenti che usufruiscono dei sistemi informatici.

Inoltre le procedure interne dovranno prevedere una check-list predefinita dove saranno evidenziati i ruoli e le attività di ogni attore che prende parte al procedimento stesso. (metodo who-does-what)

10.3. SEGNALAZIONE DEGLI EVENTI RELATIVI ALLA SICUREZZA

Gli eventi che possono creare incidenti relativi alla sicurezza delle informazioni devono essere segnalati all'Amministratore Unico tempestivamente e devono possibilmente essere documentati attraverso screenshot oppure attraverso descrizione analitica dell'evento stesso.

10.4. PROCEDURE DI SEGNALAZIONE DEI BREACH

Il Data Breach è "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" dal Titolare del trattamento.

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceasl ta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
0994585171 Uff. Finanziarie
0994585316 Uff. Amministrativo
Via Duca di Genova 63/A – 74123 Taranto
sanitaservice@asl.taranto.it
sanitaserviceasl ta@pec.it
Sede Legale: Viale Virgilio, 31 – 74123 Taranto
Sede Operativa:

In caso di furto, smarrimento, malfunzionamento o guasto, effettuare la immediata segnalazione (al massimo entro 24 ore dalla conoscenza dell'evento) al Titolare, al Designato al trattamento ed al Responsabile della Protezione dei Dati, seguendo la procedura aziendale per il Data Breach pubblicata sul sito aziendale nella sezione privacy. Tale adempimento è necessario sia per ripristinare il dispositivo, sia per ottemperare agli obblighi imposti dal Regolamento Europeo 2016/679 (eventuale notifica al Garante entro 72 ore ed agli interessati), sia per effettuare le eventuali denunce agli Enti competenti (Autorità giudiziaria, ecc.);

10.5. RACCOLTA DI EVIDENZE E REGISTRO INCIDENTI

Tutte gli incidenti saranno poi registrati dall'Amministratore di sistema su apposito registro elettronico custodito nell'archivio digitale aziendale evidenziando il nominativo dell'utente coinvolto, dell'asset, dei dati temporali e dell'evento.

11. DISASTER RECOVERY E CONTINUITÀ OPERATIVA

11.1. ATTUAZIONE DI PROCESSI DI DISASTER RECOVERY

Per quanto riguarda i processi di disaster recovery inerenti ai server aziendali si rimanda alle politiche interne dell'Asl Taranto.

11.2. ATTUAZIONE PROCESSI DI CONTINUITÀ OPERATIVA

Come sopra.

Società soggetta a direzione e coordinamento da parte dell'ASL TARANTO ai sensi dell'art. 2497 e ss. Codice Civile
www.sanitaserviceaslta.it - C.F./P.IVA 02775310739 -
0994786400 Segreteria
31 – 74123 Taranto
0994585171 Uff. Finanziarie
Via Duca di Genova 63/A – 74123 Taranto
0994585316 Uff. Amministrativo
sanitaservice@asl.taranto.it
sanitaserviceaslta@pec.it
Sede Legale: Viale Virgilio,
Sede Operativa: