DISCIPLINARE PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI DA PARTE DEGLI UTENTI

Sommario

1. SCOPO

Il presente disciplinare descrive le regole tecniche ed organizzative da applicare per l'utilizzo di strumentazioni informatiche che accedono al sistema informativo dell'Agenzia Territoriale dell'Emilia-Romagna per i servizi idrici e rifiuti (ATERSIR) di seguito denominato "Ente".

Ai fini del presente disciplinare, si intende per "sistema informativo" il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate alla acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni.

Il presente disciplinare aziendale si intende a valere anche come "istruzioni all'incaricato da parte del Titolare del trattamento" ai sensi dell'art.29 GDPR. Esso ha lo scopo di stabilire le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e collaboratori.

Pertanto, il mancato rispetto di quanto prescritto potrà costituire motivo di provvedimento disciplinare nei confronti del dipendente inadempiente.

Le disposizioni qui contenute hanno la finalità di ottimizzare l'impiego delle risorse, introdurre regole di corretto utilizzo nel contesto organizzativo dell'Ente e ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati e delle informazioni, di accesso non autorizzato o di trattamento non consentito, garantire la disponibilità dei servizi e il rispetto delle norme sul diritto d'autore.

Quanto riportato nel presente disciplinare non esaurisce tutte le prescrizioni contenute nelle vigenti normative relativamente ad illeciti disciplinari, civili e penali, con particolare riferimento alle violazioni di sicurezza e ai reati informatici.

2. CAMPO DI APPLICAZIONE

Il presente disciplinare si applica a tutti i soggetti che utilizzano i servizi del sistema informativo dell'Ente il cui accesso è consentito tramite accreditamento al sistema di gestione delle identità denominato Windows Server - Active Directory.

A mero titolo esemplificativo, rientrano nel perimetro di applicazione della presente disciplina tutti i collaboratori delle strutture e gli organi dell'Ente.

Nel seguito del disciplinare, i soggetti di cui sopra sono denominati "utenti".

3. DOTAZIONI INFORMATICHE INDIVIDUALI

In relazione al rapporto di lavoro instaurato e alle mansioni affidate, l'Ente di norma assegna agli utenti una postazione di lavoro e/o un dispositivo mobile per l'accesso alla rete e ai servizi del sistema informativo, un insieme di dotazioni software individuali e l'accesso a servizi di stampa, fotocopie e scanner con configurazione predisposta per assicurare la tutela della privacy e la riservatezza dei dati e delle informazioni trattate.

Per utenti esterni che abbiano necessità di accedere ai servizi del sistema informativo dell'Ente per le attività di assistenza/aggiornamenti dei propri applicativi, non è prevista l'assegnazione di strumentazione, ma l'accesso è garantito con l'uso di dispositivi propri, previa richiesta scritta con nomina degli utenti da società esterne che abbiano in essere contratti di servizio, e con credenziali fornite dall'Ente. Le clausole di riservatezza e garanzia vengono sottoscritte in fase di sottoscrizione del contratto di servizio (ex art. 28 GDPR)

Ogni utente è responsabile del corretto impiego delle risorse messe a sua disposizione dall'Ente.

3.1 3.1 Postazioni di lavoro

La tipologia e le caratteristiche delle postazioni di lavoro – fisse presso la sede Atersir e mobili attraverso dispositivi Atersir in uso per attività in smart working, o comunque fuori sede - sono stabilite del responsabile del Servizio gestione documentale, segreteria organi e transizione digitale, tenuto conto delle esigenze di lavoro rilevate per gruppi di utenti omogenei,

Le postazioni di lavoro hanno caratteristiche minime comuni costituite da:

- un sistema operativo omogeneo e sicuro;
- una dotazione di applicativi individuali di base omogenei e standardizzati;
- un insieme di tecnologie che abilitano all'accesso alla rete e a tutti i servizi applicativi dell'Ente, compresi eventuali certificati e/o dispositivi per il controllo delle identità del dispositivo e dell'utente;
- la possibilità di accesso da parte di Amministratori di Sistema per l'erogazione dei servizi di assistenza remota e aggiornamento automatico.

Le postazioni di lavoro sono protette, in caso di assenza anche temporanea, tramite la sospensione o il blocco della sessione di lavoro. A tale fine è impostata automaticamente l'attivazione dello screen saver in un periodo di tempo congruo e definito del responsabile del

Servizio gestione documentale, segreteria organi e transizione digitale al fine di impedire la lettura e/o la modifica dei dati presenti a video.

Allo scopo di proteggere dati personali, anche di particolari categorie e relativi a condanne penali e reati, e la sicurezza delle postazioni di lavoro, è vietato collegare supporti rimovibili o altre tipologie di dispositivi di proprietà dell'utente alle postazioni di lavoro dell'Ente.

3.2 Dotazione software della postazione di lavoro individuale

Ogni postazione di lavoro è dotata di una configurazione base costituita da software applicativi individuali e che viene tenuto, censito e aggiornato dagli amministratori di sistema.

Per i collaboratori esterni di cui al paragrafo 4.3 la fornitura della dotazione aggiuntiva di cui al capoverso precedente non è prevista

La postazione di lavoro è configurata e gestita centralmente degli amministratori di sistema (AdS) coordinati dal responsabile del Servizio gestione documentale, segreteria organi e transizione digitale nel rispetto del principio di standardizzazione di tutte le postazioni di lavoro dell'Ente.

3.3 Fotocopia e scanner

Tutti gli utenti dell'Ente possono accedere a tutte le stampanti/copiatrici multifunzione, gestite dal server centrale di controllo dei servizi di stampa e copia che garantisce i principi di stampa sicura ai fini della privacy. Le operazioni effettuate sono associate all'utente e consentono la riconducibilità di ogni stampa. È prevista una stampa con rilascio protetto da PIN per particolari tipologie di documenti riservati/coperti da privacy, definite dal dirigente competente.

3.4 Corretto utilizzo e conservazione delle dotazioni di lavoro

Le dotazioni informatiche di lavoro, insieme agli accessori fisici e alle dotazioni software individuali, devono essere:

- consegnate ad ogni nuovo utente con la configurazione standard di base aggiornata alla data di consegna;
- utilizzate e conservate con diligenza al fine di ottimizzare l'impiego delle risorse dell'Ente, il risparmio energetico e l'impatto ambientale, nel rispetto del presente Disciplinare e del Codice di comportamento dei dipendenti dell'Ente (DPR 62/2013 e delibere n. 23 e 24 del Consiglio d'Ambito);

- utilizzate in modo pertinente alle specifiche finalità della propria attività e di quelle della propria organizzazione, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi;
- custodite, anche in caso di trasferimento di sede e struttura dell'utente, insieme a tutte le altre dotazioni strumentali personali;
- restituite immediatamente in caso di cessazione del rapporto di lavoro;
- prive di dati conservati in locale al fine di usufruire del backup automatico dei dati su server.

I dati e le informazioni trattati devono essere salvati nel cloud di Google drive assegnato o su server (accessibile in VPN dall'esterno). In caso di sostituzione o guasto della postazione di lavoro, l'assistenza utenti non effettua operazioni di salvataggio di dati e informazioni salvati sui dischi locali della postazione.

Le dotazioni restituite, ritirate per riparazione o sostituite per aggiornamento della dotazione, vengono immediatamente riconfigurate in modo da cancellare ogni dato preesistente e riportate alla configurazione standard. Le dotazioni riconfigurate vengono consegnate al magazzino delle dotazioni disponibili per altri utenti.

3.5 Assistenza e interventi sulle postazioni di lavoro

Gli Amministratori di Sistema (AdS) formalmente designati, possono collegarsi in modalità remota alla postazione di lavoro, allo scopo di assicurare l'assistenza tecnica, la sicurezza e l'operatività, effettuando operazioni di manutenzione e aggiornamento del software installato. Gli interventi sono effettuati dagli Amministratori accedendo alla postazione con proprie credenziali e privilegi di Amministratore di Sistema.

Nei casi in cui l'utente segnala malfunzionamenti per la soluzione dei quali, a scopi diagnostici, è indispensabile impersonare l'utente e accedere con i privilegi allo stesso assegnati, l'intervento viene effettuato, solo su specifica richiesta e autorizzazione dell'utente stesso.

Tutte le operazioni di collegamento remoto vengono tracciate dai sistemi informatici che registrano, in maniera non alterabile, le informazioni relative all'intervento effettuato (Netwrix).

4. CREDENZIALI DI IDENTIFICAZIONE INFORMATICA E ATTIVAZIONE DEI SERVIZI

In adempimento alle misure di sicurezza previste dalla normativa vigente, si delineano di seguito le procedure e le regole d'uso per la gestione e assegnazione delle credenziali di identificazione informatica e le procedure per l'attivazione dei servizi assegnati all'utente.

L'accesso alle strumentazioni informatiche utilizzate per i trattamenti di dati personali è consentito soltanto ai responsabili o agli incaricati formalmente designati per gli specifici trattamenti di dati personali (rif. art.29 GDPR).

4.1 Credenziali di identificazione informatica

L'accesso ai dati trattati con strumentazioni informatiche avviene esclusivamente previa autenticazione, ossia tramite una procedura che verifica anche indirettamente l'identità di chi vi accede.

Le credenziali di identificazione informatica consistono in un codice per l'identificazione dell'utente, conosciuta solamente dal medesimo, oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'utente. Nello specifico:

- credenziali di identificazione informatica basate su parola chiave segreta: le credenziali userid+password utilizzate per l'accesso alle risorse dell'ente (postazioni di lavoro, server intranet, ecc.) o per l'accesso alle applicazioni con autenticazione a un fattore.

Le credenziali sono costituite da uno "userid" (composto dal nome e cognome separati da un punto) e da una password creata inizialmente e che l'utente deve modificare al primo utilizzo.. L'utente viene abilitato dall'Amministratore di dominio e, prima di poter accedere a qualsiasi risorsa informatica, deve cambiare la password.

4.2 Assegnazione delle credenziali al personale e agli amministratori dell'Ente

Il rilascio delle credenziali di identificazione informatica al personale dell'Ente (compresi gli utenti a tempo determinato e il personale comandato o in avvalimento da altre strutture pubbliche presso l'Ente), ai consiglieri e agli amministratori, è conseguente alla procedura di inquadramento giuridico da parte del Servizio competente.

Le credenziali di identificazione informatica sono concesse al personale a seguito di una procedura di accreditamento che prevede il riconoscimento "de visu".

Le credenziali di identificazione informatica sono associate ai dati con cui il personale è registrato nell'anagrafica dell'Ente e costituiscono condizione necessaria per l'abilitazione all'utilizzo dei servizi informatici.

4.3 Assegnazione delle credenziali a soggetti esterni

Qualsiasi soggetto esterno che debba accedere a tutti o a parte dei servizi di rete e di dominio direttamente presso le sedi dell'Ente o accedere tramite VPN da remoto a sistemi della rete interna, deve essere accreditato tramite il rilascio di una credenziale informatica. Il processo di rilascio delle credenziali segue quanto indicato nel paragrafo precedente. L'utente esterno potrà accedere solo ai servizi e a dati strettamente necessari e pertinenti all'incarico e al rapporto intercorrente con ATERSIR.

L'accreditamento di un soggetto esterno avviene su istanza del dirigente referente. L'istanza di accreditamento dovrà riportare per ogni soggetto da accreditare i minimi dati necessari per il rilascio delle credenziali incluso il termine di accreditamento e l'estensione dell'oggetto dell'accesso.

4.4 Gestione delle credenziali

Ogni credenziale di identificazione informatica si riferisce ad un singolo utente. Non è consentito l'utilizzo della stessa credenziale da parte di più utenti, fatti salvi i casi di userid amministrativi utilizzati da Amministratori di Sistema e di servizi di emergenza o similari in cui vi sia la necessità di consentire l'accesso ai servizi stessi senza conoscere a priori i soggetti che vi devono accedere (es. personale addetto alla gestione emergenze, ecc.); in quest'ultimo caso la struttura di appartenenza provvede a tenere aggiornato un apposito registro con l'indicazione dei nominativi, degli orari e della postazione da cui il soggetto accede.

Ogni utente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.

Ciascun utente è responsabile della sicurezza delle proprie password e deve adottare le necessarie cautele per mantenerle segrete. Le password sono infatti strettamente personali e non devono in nessun caso essere comunicate ad altri.

In caso di furto delle credenziali l'utente è tenuto a seguire le procedure di seguito specificate:

- in caso di furto della componente riservata (password o PIN) è necessario, al primo accesso seguente al furto, cambiare la propria password o pin e contattare il personale preposto alle problematiche di sicurezza informatica per darne immediatamente comunicazione.

Ciascun utente quando effettua l'accesso ad un sistema per la prima volta è tenuto a modificare e personalizzare la password di accesso che deve essere lunga almeno 12 caratteri. Si raccomanda inoltre di seguire i seguenti suggerimenti per la corretta impostazione della password:

- non impostare la password in modo che sia facilmente collegabile alla propria vita privata (per es. il nome o il cognome di familiari, la targa dell'auto, la data di nascita, la città di residenza, ecc.);
- non impostare come password parole comuni riportate in un vocabolario (esistono infatti programmi fraudolenti, utilizzati per la forzatura di password che si basano su ricerche sistematiche effettuate sulle parole comuni);
- modulare il grado di complessità della password in funzione del valore dei dati e delle risorse da proteggere; password di account con privilegi amministrativi, per esempio, richiedono complessità superiori rispetto a quelle di account non privilegiati;
- scegliere password che contengono combinazioni di lettere maiuscole e minuscole, numeri, caratteri speciali (per esempio: !, *, /, ?, #);
- **non utilizzare la medesima password su sistemi differenti** (per es. scegliere una password di dominio differente da quella impiegata per l'accesso a siti web esterni all'Ente).

La richiesta di attivazione e revoca dei servizi del sistema informativo/informatico dell'Ente e l'installazione/rimozione dei pacchetti software è di competenza del dirigente di area a cui l'utente è assegnato. Al fine di garantire la sicurezza e la responsabilità, il processo di abilitazione è tracciato in tutte le sue fasi su un sistema informatico dell'Ente ai fini dell'individuazione della responsabilità di processo.

In caso di cessazione e/o cambio di struttura dell'utente richiedente i servizi assegnati in precedenza sono di norma revocati.

In caso di sostituzione del dirigente di area, il responsabile entrante è tenuto a rivedere le assegnazioni di servizi a tutti i collaboratori interni ed esterni della struttura.

4.5 Disattivazione e cancellazione delle credenziali

Per “disattivazione delle credenziali” si intende il processo di inibizione dell’utilizzo delle credenziali e, conseguentemente, dell’accesso ai sistemi informatici e telematici dell’Ente.

Per “cancellazione delle credenziali” si intende il processo di rimozione delle credenziali dai sistemi dell’Ente e della conseguente impossibilità di utilizzo delle stesse.

Le credenziali di autenticazione assegnate al personale, agli amministratori ed ai soggetti esterni devono essere disattivate:

a) entro la mezzanotte dalla data di interruzione del rapporto di collaborazione lavorativa con l’Ente;

b) entro 7 giorni dalla eventuale segnalazione di morte o dalla dichiarazione di morte presunta;

c) nel caso non siano utilizzate da almeno 1 mese, ad eccezione di quelle utilizzate per la gestione tecnica dagli Amministratori dei Sistemi Informatici e per l’accesso ai sistemi e alle basi di dati dalle applicazioni;

d) temporaneamente, in caso di necessità e di urgenza e al fine di evitare compromissioni al normale funzionamento dei sistemi o porre termine ad attività contrarie alla normativa vigente in materia di privacy a seguito di adozione di apposito atto da parte del/i dirigente/i competente/i, fino alla rimozione delle cause che hanno originato il problema.

La riattivazione delle credenziali può essere eseguita:

1) su richiesta dell’interessato, nei casi in cui esse siano associate a un dipendente in servizio o ad un amministratore che non ne abbia fatto uso per un periodo maggiore di 1 mese;

2) su richiesta del dirigente competente nel caso di disattivazione temporanea disposta con atto del dirigente medesimo.

La cancellazione delle credenziali deve essere effettuata:

- decorsi 3 mesi dalla disattivazione delle credenziali nei casi di interruzione del rapporto di lavoro con l’Ente di dipendenti, amministratori e soggetti esterni di cui al precedente punto a);

- decorsi 3 mesi dalla disattivazione delle credenziali nei casi in cui il soggetto titolare delle stesse sia deceduto o ne sia stata dichiarata la morte presunta di cui al precedente punto b);
- decorsi 3 mesi dalla disattivazione delle credenziali per inutilizzo o per sospensione di cui ai precedenti punti c) e d), nel caso di mancata riattivazione.

4.6 Autorizzazione a risorse informatiche

La concessione del diritto di un soggetto incaricato al trattamento ad accedere a una o a più risorse informatiche dell'Ente deve essere richiesta dal dirigente competente (o persona da lui delegata per tale attività).

L'accesso alle risorse informatiche dell'Ente è consentito agli utenti abilitati in relazione al ruolo ricoperto, per il solo periodo di durata del rapporto con l'Ente e non oltre i termini di disattivazione delle credenziali.

Nel caso di cessazione del diritto di un incaricato ad accedere a una o a più risorse informatiche dell'Ente, è onere del dirigente competente (o persona da lui delegata per tale attività) assicurarsi, presso gli Amministratori dei Servizi Informatici corrispondenti, dell'avvenuta disattivazione delle autorizzazioni associate a tale incaricato.

5. UTILIZZO DI POSTAZIONI DI LAVORO PORTATILI

Il computer affidato al dipendente e/o collaboratore è uno strumento di lavoro.

Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione.

Ogni utilizzo non inerente all'attività lavorativa può contribuire a generare disservizi, costi e, soprattutto, minacce alla sicurezza aziendale.

Per i notebook e altri dispositivi mobili (tablet, smartphone etc.) forniti dall'Ente, occorre adottare comportamenti adeguati a prevenire l'accesso da parte di soggetti non autorizzati in ragione della:

- natura dei dispositivi: tali dispositivi sono facilmente trasportabili ed occultabili;
- natura dei dati presenti sui dispositivi mobili: possono essere presenti copie parziali e/o temporanee di dati personali o comunque di importanza strategica per la sicurezza dei sistemi;

- modalità di utilizzo dei dispositivi: possono essere utilizzati in contesti diversi anche al di fuori di sedi dell'Ente ed in aree non sicure e ciò rappresenta una minaccia per la sicurezza dei sistemi nel momento in cui ci si riconnette alla rete interna.

5.1 Prevenzione

Per quanto sopra precisato è fatto divieto ad ogni utente di salvare in locale credenziali che consentano l'accesso alla rete o ad applicazioni dell'Ente.

Al fine di evitare accessi non autorizzati ai dati e ai servizi dell'Ente si raccomanda di:

- provvedere, al momento della riconnessione alla rete interna dell'Ente, al salvataggio su unità di rete o sul proprio disco personale in cloud di eventuali file copiati o creati in locale, rimuovendoli dal dispositivo mobile;
- memorizzare in forma protetta i file che contengono dati sensibili e/o giudiziari (per es. proteggere l'accesso a cartelle o file tramite password, utilizzare appositi strumenti di cifratura concordandoli con il proprio referente informatico o con le strutture informatiche centrali, ecc.);
- distruggere i supporti rimovibili contenenti anche dati di particolari categorie e/o relativi a condanne penali e reati, o rendere inintelligibili i dati in essi contenuti, impiegando strumenti preventivamente concordati con il proprio referente informatico.

Per prevenire furto, danneggiamento involontario e comunque situazioni di pericolo relative all'integrità dei dispositivi e dei dati, in ragione della portabilità degli stessi, l'utente è tenuto a:

- custodire adeguatamente i dispositivi durante le ore notturne o in periodi di assenza (per es. non lasciare i dispositivi sulla scrivania ma custodirli in armadi o cassetti chiusi a chiave, dotare i portatili di dispositivi di fissaggio, ecc.);
- durante il trasporto osservare le istruzioni del fabbricante per la protezione dei dispositivi da urti, campi elettromagnetici e sbalzi di temperatura;
- trasportare i dispositivi come bagaglio a mano durante i viaggi in aereo;
- non lasciare i dispositivi incustoditi, neanche temporaneamente, durante i viaggi effettuati in treno o con altri mezzi di trasporto;
- non lasciare i dispositivi in auto, se non in casi eccezionali, e comunque chiuderli nel bagagliaio non a vista in modo da non evidenziarne la presenza dall'esterno;

- non lasciare i dispositivi in vista nelle stanze degli hotel, ma chiuderli in un armadio o in una valigia o depositarli in cassaforte se si prevede un'assenza prolungata.

I computer portatili ad uso individuale devono essere utilizzati esclusivamente dall'utente a cui gli stessi sono stati assegnati e, qualora siano assegnati alle strutture, il loro utilizzo deve essere regolamentato dalle stesse, in funzione delle proprie peculiarità ed in modo tale da garantirne il controllo.

Gli utenti assegnatari provvedono al collegamento delle postazioni di lavoro portatili alla rete dell'Ente almeno una volta ogni 30 giorni per effettuare gli aggiornamenti automatici del software antivirus e delle patch di sicurezza del sistema operativo e di tutti i prodotti software installati. Se l'utente assegnatario utilizza il dispositivo mobile per smartworking, lo stesso è tenuto ad osservare le disposizioni illustrate nel paragrafo relativo.

5.2 Dispositivi smartphone e tablet forniti dall'Ente

I dispositivi mobili, in ragione della loro natura, rappresentano una minaccia rilevante alla confidenzialità dei dati e delle informazioni dell'Ente. Specificatamente i dispositivi mobili sono soggetti a rischi specifici quali perdita di informazioni, accesso a dati "sensibili", facilità di furto, accesso a reti wireless non sicure, possibilità di download di app con contenuto malevolo.

La gestione dei dispositivi mobili assegnati dall'Ente a collaboratori e amministratori avviene attraverso una procedura che ha lo scopo di monitorare la sicurezza di tali dispositivi e di determinare centralmente il rispetto di parte delle policy qui descritte.

Per ridurre il livello di esposizione alle minacce viene stabilito che:

- Ogni utente che riceve in dotazione un dispositivo mobile è responsabile del suo corretto utilizzo;
- Ogni utente, oppure il personale tecnico addetto alla gestione dei dispositivi mobili dell'Ente, attiva l'impostazione del blocco dello schermo dopo pochi minuti di inattività (interazione utente- device) con sblocco attraverso password;
- Il personale tecnico addetto alla gestione dei dispositivi mobili dell'Ente installa sul dispositivo mobile un software anti malware il cui database è aggiornato continuamente (database definizione virus);
- È fatto divieto all'utente di effettuare la disinstallazione, la disattivazione o qualsiasi manipolazione del software anti malware installato; l'utente inoltre è tenuto a consentire l'aggiornamento del software anti malware attraverso la connessione dati;

- È fatto divieto all'utente di installare software che comporti rischi per la sicurezza e di modificare funzionalità del sistema operativo del dispositivo mobile attraverso operazioni di “rooting” o “jailbreaking”;
- L’accesso via VPN alla rete dell’Ente attraverso il dispositivo mobile deve essere esplicitamente autorizzata del responsabile del Servizio gestione documentale, segreteria organi e transizione digitale.
- Al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile, sia all'interno che all'esterno degli uffici dell’ente, riponendolo in cassetti o armadi chiusi a chiave in caso di non utilizzo;
- In caso di furto o smarrimento del dispositivo, l'utente è tenuto a segnalarlo tempestivamente al servizio che gestisce il dispositivo, in modo che gli incaricati della gestione dei dispositivi mobili dell’Ente provvedano, qualora possibile, alla cancellazione remota dei dati contenuti all'interno (“remote wiping”); l'utente deve inoltre effettuare la denuncia presso le autorità competenti e farne pervenire copia al servizio che gestisce il dispositivo mobile.
- Poiché i dispositivi mobili sono utilizzati su reti di cui l'Ente non ha nessun controllo, con conseguente rischio di intercettazione e/o di modifica delle comunicazioni effettuate con tali dispositivi, l'utente è invitato ad utilizzare i cellulari di servizio in hotspot o reti Wi-Fi con accesso tramite autenticazione.
- Il personale tecnico addetto alla gestione dei dispositivi mobili dell’Ente è tenuto ad effettuare un audit periodico delle attività effettuate dagli utenti possessori di dispositivi mobili, anche attraverso uno strumento MDM (Mobile Device Management), allo scopo di individuare accessi non autorizzati ai dati, violazioni delle policy e compromissioni dei dispositivi. Tale audit viene effettuato senza alcuna comunicazione preventiva all’utente, nell'interesse della tutela del patrimonio informativo dell'Amministrazione e della sicurezza delle informazioni degli utenti.
- Salvo specifica richiesta dell’Autorità giudiziaria la funzione degli strumenti di MDM che consente il tracciamento della posizione fisica in cui si trova il dispositivo (geolocalizzazione), è disattivata.

5.3 Smart Working

La modalità di lavoro definita smart working prevede che ai dipendenti autorizzati dall'Ente venga assegnata una postazione di lavoro portatile (se non già assegnata per lo svolgimento delle attività lavorative in modalità ordinaria) da utilizzarsi presso una sede differente dalla sede aziendale assegnata per lo svolgimento delle proprie attività lavorative.

I dipendenti sono autorizzati ad utilizzare ulteriore strumentazione aziendale (es. telefono mobile) qualora già assegnata. Potranno inoltre far uso di propria strumentazione personale (es. telefono fisso o mobile) sotto la propria esclusiva responsabilità.

Alla strumentazione in dotazione si applicano le medesime policy relative agli smartphone e tablet descritte al paragrafo 5.2.

5.4 5.4 Utilizzo dei dispositivi non forniti dall'ente

I soggetti accreditati al dominio dell'Ente hanno accesso ai servizi dell'Ente esposti sulla rete esterna o resi disponibili in modalità cloud, pertanto fruibili attraverso una pluralità di dispositivi.

Al fine di mantenere la sicurezza dei dati di proprietà dell'Ente, trattati attraverso tali dispositivi, è necessario che l'utente adotti gli accorgimenti e gli strumenti necessari per garantire la riservatezza, l'integrità e la disponibilità dei dati memorizzati sull'infrastruttura informatica dell'Ente, prevenendone la memorizzazione insicura ovvero la loro trasmissione attraverso una rete insicura, dove possono essere facilmente compromessi. Obiettivo di queste disposizioni è anche la tutela dell'utente stesso che adottando i comportamenti indicati non incorre in violazioni delle normative vigenti e in attribuzioni di responsabilità.

L'utente che accede ai servizi aziendali fuori dalla rete dell'Ente è tenuto a:

- non memorizzare dati dell'Ente su dispositivi personali, soprattutto nel caso di documenti classificati come "confidenziali" o "strettamente confidenziali" e nel caso di presenza di dati personali (in particolare dati di particolari categorie e/o relativi a condanne penali e reati) e a non scaricare in locale gli allegati di posta elettronica. Nel caso in cui i dati dell'Ente venissero inavvertitamente salvati sul dispositivo personale, l'utente è tenuto a cancellarli immediatamente dal dispositivo;
- impostare il blocco automatico dello schermo del dispositivo dopo pochi minuti di inattività (interazione utente-device) con sblocco attraverso password, pin o riconoscimento biometrico;

- installare sul dispositivo un software anti malware con aggiornamento costante del database di definizione dei malware (a titolo esemplificativo di software gratuiti Avast, Malwarebytes, Avira, AVG);
- utilizzare in via esclusiva il dispositivo configurato per l'accesso a dati dell'Ente, quindi senza condividerne l'utilizzo con altri soggetti, compresi i propri familiari;
- mantenere aggiornato il dispositivo, applicando tutte le patch di sicurezza, upgrade del sistema operativo e aggiornamenti delle applicazioni installate;
- non installare sul dispositivo applicazioni provenienti da fonti non ufficiali e/o potenzialmente pericolose per l'integrità e la sicurezza dei dati dell'Ente;
- non utilizzare sul dispositivo lo stesso client per accedere sia alla posta elettronica aziendale che a quella personale ovvero per accedere ai documenti dell'Ente disponibili in cloud.

5.5 Utilizzo di smartphone e tablet personali per l'accesso a dati e servizi dell'Ente

È possibile accedere ad alcune delle risorse dell'Ente a mezzo di smartphone e tablet anche di proprietà personale, sia nel caso in cui la SIM card sia di proprietà personale, sia nel caso in cui la SIM card sia fornita dall'Ente.

Per questi casi, oltre a quanto già prescritto nel paragrafo precedente, si stabilisce che:

- I protocolli consentiti per l'accesso alla posta elettronica da smartphone e tablet sono in IMPAT con account Google Workspace Enterprise Standard.
- La configurazione dell'account aziendale sull'app nativa per la gestione della posta elettronica è subordinata all'accettazione del fatto che il sistema di gestione del servizio di posta elettronica dell'Ente, per funzionare, necessita di acquisire il controllo del dispositivo al fine di poter attuare attività avanzate di gestione, anche remota, del dispositivo mobile. Tra gli strumenti avanzati per la gestione remota si segnala la possibilità – in caso di furto o smarrimento - di effettuare il "remote wiping". Questo consente di rimuovere i contenuti personali ed aziendali dal dispositivo rubato o smarrito. L'operazione viene svolta direttamente dall'utente con il supporto assistito dello staff tecnico del responsabile del Servizio gestione documentale, segreteria organi e transizione digitale.
- **L'utente è tenuto ad impostare il blocco automatico dello schermo dopo pochi minuti di inattività con sblocco attraverso password, PIN o riconoscimento biometrico.**

- L’utente è tenuto ad installare sul proprio dispositivo mobile, sempre ove possibile, un software antimalware.
- L’utente è tenuto a non installare app al di fuori dei canali di distribuzione ufficiali (Google Play, Microsoft Store o Apple Store, c.d. “Sideloading”) e a non installare app non compatibili con la sicurezza dei dati.
- Al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile.
- L'utente deve inoltre effettuare la denuncia presso le autorità competenti e far pervenire una copia della denuncia al responsabile del Servizio gestione documentale, segreteria organi e transizione digitale.
- Nel caso in cui l’utente sospetti una violazione dei dati dell’Ente, la presenza di un malware, oppure la compromissione del proprio dispositivo mobile personale utilizzato per accedere ai dati dell’Ente, è tenuto a segnalarlo tempestivamente al responsabile del Servizio gestione documentale, segreteria organi e transizione digitale, in modo che, se fosse confermata una compromissione di dati dell’Ente, possano essere attivate opportune contromisure al fine di limitare i danni.
- Poiché i dispositivi mobili sono utilizzati su reti di cui l'Ente non ha nessun controllo, esiste un rischio di intercettazione e/o di modifica delle comunicazioni effettuate con tali dispositivi. Per tali motivi l'utente è invitato ad utilizzare preferibilmente reti Wi-Fi con accesso tramite autenticazione.

6. UTILIZZI DELLA RETE DELL’ENTE

Al fine di prevenire l’accesso ai sistemi informatici da parte di soggetti non autorizzati, alla rete ATESIR vengono collegati apparati di cui sia stato registrato il MAC ADDRESS del pc/notebook o del dispositivo di connessione; è comunque fatto divieto di:

- connettere ad Internet, tramite reti wi-fi, modem o altri apparati di accesso remoto non espressamente autorizzati, strumentazioni informatiche collegate alla rete interna dell'Ente;
- connettere alla rete interna dell'Ente strumenti elettronici personali o comunque non espressamente autorizzati;
- connettere alla rete interna dell’Ente access point o altri apparati di rete non espressamente autorizzati;

- installare e/o comunque utilizzare software peer-to-peer o utilizzare le postazioni di lavoro collegandole tra loro per la condivisione di file e stampanti;
- utilizzare strumenti di sniffing, cracking o scanning e introdurre o diffondere volontariamente programmi nocivi (per es. virus, worm, spyware, ecc.) nella rete o nei sistemi.

7. POSTA ELETTRONICA

La casella di posta elettronica viene fornita dall'Ente quale strumento di supporto per lo svolgimento dell'attività lavorativa e delle attività che siano strumentali e connesse alla stessa.

La casella di posta personale, assegnata dall'Agenzia all'utente, è uno strumento di lavoro di proprietà dell'Ente.

Le caselle di posta elettronica sono assegnate come servizio di base a ciascun dipendente e amministratore al momento dell'inquadramento giuridico e a ciascuna Area o servizio dell'Ente che ne faccia richiesta, come "Gruppo di Google".

Ai collaboratori esterni accreditati al dominio dell'Ente la casella di posta è assegnata su richiesta motivata del Responsabile della struttura qualora risulti indispensabile per svolgere attività che non risulta possibile svolgere con email personali e/o aziendali. La richiesta di attivazione dei servizi di posta personale dell'Ente ai collaboratori esterni accreditati segue le procedure di attivazione precedentemente descritte.

L'attivazione di ulteriori caselle di posta elettronica, per attività di gruppo o di progetto, può essere richiesta al responsabile del Servizio gestione documentale, segreteria organi e transizione digitale dal Dirigente dell'area con le procedure attivazione precedentemente descritte.

Le caselle di posta elettronica certificata (PEC) non sono nominative, ma assegnate alle AOO dell'Ente per le quali sono previsti processi di comunicazione istituzionale con soggetti terzi. La richiesta di attivazione di caselle PEC segue le procedure di attivazione precedentemente descritte.

Al fine di assicurare la disponibilità dei dati e delle informazioni pervenute o inviate dalle caselle di posta elettronica si raccomanda la creazione e l'utilizzo di caselle di posta elettronica di struttura e/o di progetto condivise tra gli utenti che concorrono alle suddette attività.

L'amministrazione degli utenti che accedono a caselle di struttura, di gruppo o di progetto è assegnata all'amministratore di sistema

ATERSIR, in qualità di Titolare del trattamento di dati personali informa ogni dipendente e collaboratore a cui sia stata assegnata una casella email aziendale nominativa che:

- l'accesso a tale casella – in quanto nominativa – è consentito esclusivamente alla persona a cui la casella stessa è stata assegnata;
- ogni utente è responsabile della riservatezza della propria casella email e deve quindi adottare le opportune misure per evitare che altri (anche colleghi) abbiano accesso alla casella;
- l'accesso alla casella potrà essere permesso a colleghi o altre figure aziendali (c.d. fiduciario), solo a fronte di motivate e concordate esigenze lavorative aziendali (per esempio in caso di prolungata assenza del titolare della casella); quando tale esigenza sarà cessata, il titolare della casella dovrà provvedere al cambio della password di accesso;
- l'Ente non accede alle caselle di posta nominative dei dipendenti e collaboratori, ma informa che solo ed esclusivamente al verificarsi di documentate esigenze aziendali potrà eseguire – motivandolo – l'accesso alla casella di posta nominativa del dipendente; in tale evenienza il dipendente sarà informato e gli saranno indicati i motivi che hanno giustificato tale accesso.

I motivi che possono legittimare l'Ente all'accesso ed al controllo di una casella email nominativa individuale sono, a titolo esemplificativo ma non esaustivo: indagini forensi a seguito di incidente informatico, anomalie riscontrate sul sistema informatico aziendale, sospetti di violazione delle regole aziendali con potenziale danno all'Ente, controlli difensivi a tutela dell'Ente, evitare la distruzione di informazioni necessarie per lo svolgimento di un procedimento disciplinare, su richiesta del soggetto titolare del procedimento stesso.

7.1 Utilizzo della posta elettronica

La posta elettronica deve essere utilizzata esclusivamente per le specifiche finalità della propria attività lavorativa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi e degli altri utenti dell'ente e dei processi lavorativi, adottando comportamenti idonei a prevenire la perdita di confidenzialità di dati riservati e l'utilizzo non appropriato di beni e servizi dell'Ente.

La casella di posta elettronica certificata (PEC) e quella ordinaria sono mezzi attraverso i quali è possibile la trasmissione di dati personali. Nei casi in cui siano utilizzati quali mezzi per trasmettere dati personali a soggetti terzi, si rammenta che tale operazione costituisce

comunicazione di dati personali e, come tale, deve essere effettuata ai sensi della normativa vigente oppure a riscontro di una istanza dell'interessato ai propri dati personali.

Nel caso di utilizzo della posta elettronica certificata (PEC) per la trasmissione di dati personali comuni (vale a dire non particolari, ovvero non dati di particolari categorie e/o relativi a condanne penali e reati) il cui trattamento sia di titolarità dell'Ente, l'utente dovrà solo accertarsi della legittimità del destinatario a ricevere i dati personali che intende inviare; qualora venisse utilizzata, invece, la casella di posta elettronica "ordinaria" l'utente dovrà accertarsi, oltre che della legittimità del destinatario alla ricezione dei dati personali, anche dell'identità dello stesso, che si intende certa se:

- ha presentato via email una richiesta per l'invio dei dati firmata digitalmente;
- oltre alla richiesta di dati presentata via email o telefonicamente, ha trasmesso, anche via mail, una copia semplice di un documento di identità in corso di validità.

Nel caso di ragionevole certezza sull'identità del richiedente (ad esempio perché il richiedente è conosciuto personalmente) ovvero in casi di improrogabile urgenza, l'accertamento sull'identità del ricevente può essere effettuata per via telefonica.

Le modalità tecniche cambiano in relazione alla tipologia dei dati personali che si intende inviare.

Nei casi in cui sia necessario inviare dati ascrivibili a particolari categorie di dati personali (rif. art.9 GDPR) e/o relativi a condanne penali e reati (rif. art.10 GDPR), verificata da parte dell'utente la liceità del trattamento ai sensi della normativa vigente, la comunicazione deve essere effettuata secondo una delle seguenti modalità:

- utilizzando opportune tecniche di cifratura avvalendosi di strumenti preventivamente concordati con il proprio referente informatico o con le strutture informatiche centrali;
- impiegando soluzioni alternative che rendano i dati temporaneamente inintelligibili e permettano di identificare gli interessati solo in caso di necessità (per es. mandare in email separate i dati di particolari categorie e/o relativi a condanne penali e reati dagli altri dati personali, utilizzare codici identificativi al posto di nome e cognome, ecc.).

7.2 Prevenzione da malware

Al fine di prevenire le minacce rappresentate da software malevoli (per es. virus, worm, spyware, ransomware ecc.) che potrebbero essere contenuti in email o negli allegati delle email stesse, si forniscono le seguenti indicazioni:

1. “Spam” è il termine con cui si indica l'invio incessante, ma soprattutto indesiderato di messaggi pubblicitari o parti delle cosiddette catene di S. Antonio ad un gran numero di utenti contemporaneamente. Le operazioni di invio possono realizzarsi via email o tramite i gruppi di discussione.
2. A titolo preventivo si raccomanda di:
    - non rispondere mai a messaggi di presunto spamming, neppure se al momento della cancellazione della mail viene richiesta conferma di lettura dal mittente, poiché ciò consente al mittente di verificare l'effettiva esistenza dell'indirizzo di posta dell'utente;
    - limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail su siti web pubblici (per es. forum, mailing list, ecc.);
    - non utilizzare l’account email aziendale per registrarsi a siti/servizi web che non siano necessari per l’attività lavorativa e/o che siano per un uso personale;
    - non rispondere o inoltrare email di c.d. “Catene di S. Antonio”, ovvero messaggi dal contenuto ambiguo che esortano ad inoltrare urgentemente delle copie ad altre persone;
    - non configurare la conferma di lettura in modalità automatica.
3. Il phishing è una tecnica di attacco che sfrutta email e siti web “clonati”, del tutto simili nell’aspetto agli originali, per ingannare l’utente e carpire informazioni confidenziali o personali. È necessario, quindi, prestare massima attenzione alle email che richiedono di fornire dati riservati quali password o numeri di carta di credito, attraverso la compilazione di moduli web (per es. da parte di una banca, di un operatore telefonico, di studi legali o di fornitori di servizi quali Yahoo!, Poste, ecc.).
4. Anche nel caso di messaggi provenienti da mittenti conosciuti, ma che contengono allegati sospetti (file con estensione.exe.scr.pif.bat.cmd, file di tipo di tipo Office contenenti macro), questi ultimi devono essere verificati attentamente con l’ausilio dei Sistemi informativi dell’Ente, prima di essere aperti.
5. In caso di dubbi sulla qualità di messaggi email, si raccomanda di contattare l'indirizzo di posta dedicato alle problematiche di sicurezza informatica dell’Ente (help@atersir.it).

8. NAVIGAZIONE IN INTERNET

L'Ente fornisce l'accesso a Internet a supporto dello svolgimento dell'attività lavorativa e delle attività che siano strumentali e connesse alla stessa e per questo se ne prescrive un utilizzo pertinente alle specifiche finalità, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi.

È fatto divieto di:

- modificare le configurazioni standard del browser web fornito dall'Ente;
- accedere dal computer aziendale a caselle web mail di posta elettronica personale;
- scaricare o eseguire alcun software o altro contenuto attivo, anche se gratuito, da siti Internet se non per finalità istituzionali e solo se strettamente necessario. In tal caso, lo scaricamento di tale software deve essere preventivamente autorizzato dagli amministratori di sistema dell'Ente;
- utilizzare siti pubblici di condivisione dei file e di archiviazione online forniti da provider che non assicurano strumenti di protezione adeguati;
- caricare documenti inerenti all'attività lavorativa o istituzionale, soprattutto se contenenti dati personali, di particolari categorie e/o relativi a condanne penali e reati, su siti pubblici di condivisione, archiviazione o backup online.

Per contrastare le nuove tipologie di attacco informatico che hanno come obiettivo l'utente finale e come mezzo di propagazione il web o la posta elettronica, e le comunicazioni web che utilizzano sempre più frequentemente canali cifrati, il personale del responsabile del Servizio gestione documentale, segreteria organi e transizione digitale addetto alla sicurezza informatica è autorizzato a configurare sistemi di sicurezza dedicati alla navigazione web, per ispezionare il traffico cifrato nei siti ritenuti ad alto rischio (tipicamente quelli che permettono lo scambio di documenti) allo scopo di individuare e bloccare eventuale malware o strumenti di attacco. Tale ispezione, funzionale unicamente alla verifica della sicurezza delle informazioni, è effettuata con strumenti automatici; per nessun motivo viene utilizzata per il controllo dell'attività lavorativa.

9. PROTEZIONE ANTIVIRUS

L'utente utilizzatore delle risorse informatiche dell'Ente è tenuto ad adottare le necessarie cautele al fine di ridurre il rischio di infezione virale della propria o altrui postazione di lavoro. È fatto quindi divieto, ai soggetti che sono amministratori di postazione di lavoro, di rimuovere

il programma antivirus installato su di essa e di alterarne la configurazione. Si invitano gli utenti a segnalare problemi eventualmente riscontrati sulla corretta installazione e funzionamento del programma antivirus installato sulla propria postazione di lavoro.

Si raccomanda, inoltre, prima di utilizzare supporti rimovibili (quali chiavette USB), di verificare la presenza di eventuali virus in esso contenuti.

A seguito di segnalazione della presenza di un virus da parte del software antivirus si prescrive di:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare tramite mail l'evento al responsabile del Servizio gestione documentale, segreteria organi e transizione digitale ;
- non inviare ad altri utenti i messaggi di posta elettronica contenenti segnalazioni del virus.

10. GESTIONE DEI LOG

I sistemi informativi dell'Ente sono verificati sia periodicamente sia su segnalazione di incidenti di sicurezza, allo scopo di garantirne l'efficienza, la disponibilità ed il rispetto di leggi e regolamenti, ed in particolare dei requisiti di sicurezza previsti dalla normativa vigente in materia di protezione dei dati personali.

Alcune attività dell'utenza sono soggette a logging: ciò significa che alcune operazioni eseguite dagli utenti di sistemi informativi vengono memorizzate in formato elettronico e conservate per un certo periodo di tempo. Il logging è necessario per ragioni di sicurezza: il livello del logging dei diversi servizi, ossia il livello di dettaglio dei dati memorizzati, è funzionale unicamente alla verifica della sicurezza con la quale i servizi sono erogati e per nessun motivo viene utilizzato per il controllo dell'attività lavorativa.

Di seguito vengono dettagliate le tipologie di log raccolti e conservati:

- log della navigazione web, del firewall e del server di posta: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze; scopo ulteriore della raccolta, per quel che riguarda la navigazione web, è quello di verificare il corretto utilizzo delle strumentazioni assegnate dall'Ente al fine di svolgere la propria attività lavorativa;

- log delle segnalazioni ed alert di tutte le tipologie di sistema antimalware: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log degli accessi degli Amministratori di Sistema ai sistemi amministrati: tale raccolta è motivata dalla necessità di ottemperare al Provvedimento del Garante per la Protezione dei dati personali relativo agli Amministratori di Sistema;
- log degli accessi degli utenti ai servizi di rete: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log degli accessi degli utenti al sistema di stampa e delle operazioni effettuate: tale raccolta deriva dalla necessità di poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze; scopo ulteriore della raccolta è quello di verificare il corretto utilizzo delle strumentazioni assegnate dall'Ente al fine di svolgere la propria attività lavorativa;
- log delle attività svolte da utenti e amministratori di sistema nell'ambito di alcuni software complessi: tale raccolta è motivata dalla necessità di poter individuare anche a posteriori eventuali violazione delle policy e audit sulla correttezza dei dati gestiti dal software stesso.

Il tempo di conservazione di tutte le tipologie di log sopra elencate è fissato ad un periodo di un anno oppure di un periodo superiore nei casi previsti dalle normative. Ciò è motivato dalla necessità di utilizzare tali log per la verifica annuale delle attività degli amministratori di sistema prevista dal provvedimento del Garante per la Protezione dei dati personali e di avere una policy di retention dei log uniforme per tutte le tipologie, in modo da semplificare ed economizzare la gestione del sistema dei log e delle politiche di backup.

11. PREVENZIONE E GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

Al fine di prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile è di enorme rilevanza operare tempestivamente e in uno spirito di collaborazione.

Qualora si ravvisassero violazioni di sicurezza interna o eventi che possano portare a credere che vi sia stata una elusione delle misure di sicurezza previste, è di fondamentale rilevanza

segnalare tempestivamente l'accaduto al referente ICT di riferimento / struttura competente in materia di ICT dell'Ente. Si rinvia alla Detetermina n. 176 del 26 luglio 2023 - Data Breach per segnalare eventuali rischi o sospette violazioni secondo la procedura ivi prevista.

In un'ottica di prevenzione degli incidenti di sicurezza, è necessario attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi. Tali indicazioni sono fornite agli utenti attraverso gli strumenti di comunicazione interna dell'Ente.

12. PROTEZIONE DEI DATI TRATTATI SENZA L'UTILIZZO DI STRUMENTI ELETTRONICI

L'accesso ai dati trattati senza l'utilizzo di strumenti elettronici è consentito, come per i trattamenti di dati personali effettuati con mezzi elettronici, esclusivamente al personale espressamente incaricato.

Vi sono, inoltre, alcuni basilari comportamenti che, se messi in atto, riducono in maniera considerevole i rischi di accesso ai dati da parte di persone non autorizzate, di perdita di confidenzialità dei dati e della conseguente mancanza di disponibilità degli stessi.

In linea con quanto sopra, è assolutamente necessario raccogliere prontamente, nel caso si utilizzino stampanti di rete in locali comuni (per es. corridoi), i documenti stampati - e se contenenti dati personali prevedere la stampa tramite rilascio con pin - in modo da preservarne la riservatezza del contenuto. È ugualmente rilevante, ai fini della tutela dei dati personali trattati nell'espletamento delle proprie mansioni, assicurarsi, al termine della giornata lavorativa, che i documenti contenenti dati personali o rilevanti ai fini della sicurezza del sistema informativo dell'Ente, non siano lasciati a vista sulla scrivania ma conservati in cassetti o armadi. Conseguentemente e al fine di non eludere tali precauzioni, è opportuno conservare con le dovute cautele le chiavi dei cassetti e degli armadi.

E' inoltre utile prevedere la disponibilità delle stesse, durante la propria assenza dall'attività lavorativa, in modalità controllata e sicura (esempio: copia delle chiavi depositate in segreteria, registro di presa in carico e di riconsegna, etc.).

Nei casi in cui atti o documenti contengano dati di particolari categorie e/o relativi a condanne penali e reati, si raccomanda di prevedere apposita procedura per la conservazione in archivi ad accesso selezionato, disciplinando modalità di ingresso tali da consentire l'identificazione degli utenti che vi accedono. Conseguentemente si sottolinea la necessità di custodire opportunamente i documenti prelevati per impedire l'accesso improprio da parte di persone

non autorizzate. In particolare, essi non dovranno rimanere incustoditi nemmeno per brevi periodi, provvedendo eventualmente a riporli in armadi o cassetti chiusi a chiave. Al termine del trattamento, l'utilizzatore avrà cura di ricollocare i documenti nell'archivio di provenienza. Tali cautele sono individuate nel Manuale per la gestione documentale adottato con Determinazione n. 44 del 02 marzo 2021.

13. RECUPERO DEI DATI DA PARTE DELL'ENTE IN ASSENZA DELL'UTENTE E INDICAZIONE DEL FIDUCIARIO

In questo paragrafo, che richiama quanto già espresso al cap. 7. Posta elettronica, sono individuate apposite procedure volte a:

A. permettere all'Ente di recuperare dati, informazioni o documenti trattati nell'espletamento delle attività lavorative di un dipendente o di un collaboratore, nei casi in cui l'assenza dello stesso sia programmata (ad esempio per ferie) oppure sia improvvisa e imprevista (ad esempio per malattia);

B. abilitare altri collaboratori (ad es. gli addetti ad una segreteria) all'utilizzo della casella di posta elettronica pur in presenza del titolare della casella stessa (ad es. il dirigente di struttura).

Tali procedure sono volte a bilanciare nel caso di cui alla lettera A), il diritto dell'Ente a garantire l'operatività organizzativa e amministrativa e l'uso consono degli strumenti forniti agli utenti con il diritto del lavoratore alla tutela della propria sfera di riservatezza anche nell'ambito della propria attività lavorativa.

È poi prevista una specifica procedura nel caso di cessazione del rapporto di lavoro.

Nel pieno rispetto del Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" e degli orientamenti sia del Garante stesso sia giurisprudenziali in materia, con le procedure di seguito esplicitate sono disciplinati in maniera esaustiva i casi in cui i dati relativi all'attività lavorativa del dipendente e del collaboratore dell'Ente possano essere conosciuti dall'Ente nell'esercizio delle proprie prerogative organizzative. La priorità è concessa a modalità e strumenti che non comportano un accesso diretto ai dati personali e alle informazioni trattate dall'utente e quindi a funzionalità che meno comprimono il diritto alla riservatezza.

In aderenza alle indicazioni del Garante con il Provvedimento suindicato e la successiva normativa e giurisprudenza, figura centrale delle procedure di seguito specificate è il

"fiduciario". Questi è un soggetto scelto liberamente da ciascun utente, che ha il compito di assicurare l'accesso ai dati trattati dall'utente fiduciante solo nei casi di assenza dello stesso. Quest'ultimo è ovviamente tenuto ad avvisare preventivamente il fiduciario e a comunicarne l'indicazione nominativa all'Ente, che ha l'onere di tenere aggiornato l'elenco dei fiduciari. A titolo esemplificativo il "fiduciario" potrebbe essere un collega che collabora nello stesso settore di attività lavorativa del fiduciante oppure che conosce o partecipa a un determinato progetto insieme al fiduciante stesso. La possibilità di indicare un fiduciario è una facoltà e non un obbligo per l'utente.

Il fiduciario, comunque, può accedere ai messaggi di posta oppure a files e cartelle del fiduciante soltanto nel caso in cui l'utente fiduciante stesso abbia, in caso di assenza programmata, attivato nei suoi confronti la funzione di delega ai messaggi della propria casella di posta elettronica oppure lo abbia autorizzato all'accesso a files e cartelle presenti nello spazio cloud personale.

Negli altri casi, qualora l'utente non abbia designato un proprio "fiduciario" e/o non abbia attivato alcuna funzione di delega all'accesso, la possibilità di accedere a suoi messaggi di posta oppure a files o cartelle presenti nello spazio personale in cloud o sulle risorse di rete, può avvenire soltanto in casi di effettiva e improrogabile necessità di assicurare continuità all'attività lavorativa. Soltanto in tale caso di emergenza sono previste e di seguito esplicitate le procedure che contemplano l'accesso alla casella di posta elettronica e ai dati dello spazio personale dell'utente su istanza del Responsabile della Struttura di appartenenza e per mezzo dei referenti informatici dell'Ente

È comunque fatto divieto allo stesso fiduciario o ad altro utente eventualmente delegato o autorizzato di accedere ai messaggi di posta elettronica e a file o cartelle che, già dall'oggetto e/o dalla denominazione e/o dalle proprietà, possano far prefigurare un contenuto riconducibile a informazioni personali non riconducibili ad attività lavorativa che, anche in tale sede, devono ricevere la dovuta tutela.

La nomina del fiduciario è strumento centrale e rilevante anche in ragione del fatto che l'Ente non utilizza risposte automatiche "Utente Fuori Sede" verso indirizzi di posta elettronica esterni, in quanto tale soluzione comporterebbe la segnalazione del dominio dell'Ente di posta nelle Black List di Reputation: l'immediata conseguenza di ciò sarebbe il blocco della ricezione delle mail provenienti dall'Ente da parte dei sistemi di posta elettronica esterni.

È fatto divieto di conservare cartelle e documenti di lavoro sui dischi locali dei personal computer, dei portatili e di smartphone e tablet. Ciò comporterebbe, altrimenti, l'assunzione di

rischi elevati in termini di confidenzialità, integrità e disponibilità dei contenuti prodotti da ciascun utente e, pertanto, deve essere limitata a operazioni su copie temporanee di lavoro.

Nei casi in cui l'Ente abbia necessità di accedere a contenuti necessari ad assicurare la continuità dell'attività lavorativa che l'utente abbia incautamente memorizzato sul disco locale della postazione di lavoro assegnata, si applicano per analogia le regole stabilite nei paragrafi seguenti.

13.1 Recupero dati in caso di assenze programmate

In caso di assenze programmate (ad esempio in caso di ferie) e qualora vi siano esigenze di assicurare la continuità dell'attività lavorativa, l'utente condivide:

- l'accesso in delega ai propri messaggi di posta elettronica a mezzo del software in utilizzo;
- file o cartelle a mezzo del cloud o delle risorse di rete;

in favore del proprio fiduciario oppure in favore di altro soggetto, (ad es. quando lo stesso fiduciario è assente).

Il fiduciario o comunque il soggetto delegato farà accesso ai soli messaggi di posta elettronica o file/cartelle necessari ad assicurare la continuità dell'attività lavorativa.

Lo stesso "fiduciario" (o il delegato) può comunicare ai mittenti dei messaggi ricevuti nella casella di posta dell'utente assente, l'assenza dell'utente "fiduciante", e che, sino ad una determinata data, sarà lui stesso a prendere visione dei messaggi inviati su quella casella di posta.

13.2 Recupero dati in caso di assenze non programmate con indicazione del fiduciario

In caso di assenze non programmate, come ad esempio per malattia, e qualora l'utente non abbia attivato le funzioni di condivisione descritte nel paragrafo precedente, il Responsabile della Struttura di appartenenza dell'utente assente, esclusivamente per effettiva e improrogabile necessità di assicurare continuità all'attività lavorativa, richiede al Responsabile del responsabile del Servizio gestione documentale, segreteria organi e transizione digitale di attivare la funzione di delega all'accesso alla casella di posta elettronica o al cloud o alle risorse di rete assegnato all'utente assente. La funzione di delega sarà attivata in favore dell'utente designato preventivamente quale "fiduciario" dall'utente assente.

L'istanza di accesso deve essere trasmessa anche in copia all'utente assente e al fiduciario dallo stesso nominato.

La funzione di delega su descritta rimane attiva per il tempo strettamente necessario al recupero dei contenuti e delle informazioni che si reputano indispensabili per dare continuità all'attività lavorativa dell'Ente oppure per un periodo di tempo limitato (quale ad esempio quello della malattia dell'utente assente) al termine del quale la funzione di delega è automaticamente disattivata.

Dopo aver effettuato l'accesso alla casella del collega "fiduciante" e dopo aver trasmesso al Responsabile di Struttura istante i messaggi di posta elettronica richiesti, di tali operazioni l'utente fiduciario redige verbale delle operazioni effettuate che consegnerà agli atti della struttura affinché anche l'utente stesso possa prenderne visione al rientro.

13.3 Recupero dati in caso di assenze con mancata indicazione del fiduciario

Qualora l'utente assente non avesse provveduto a individuare un proprio "fiduciario" e non avesse delegato neppure altri soggetti ad accedere ai propri contenuti, si prevede, sia nel caso in cui l'assenza sia programmata sia nel caso in cui non lo sia, che:

A. il Responsabile della Struttura di appartenenza dell'utente assente che esclusivamente per le succitate esigenze intende accedere a messaggi (inclusi gli eventuali allegati) presenti nella casella di posta elettronica o a file/cartelle presenti nel cloud assegnato, o sulle risorse di rete, allo stesso, deve effettuare la richiesta al Responsabile del responsabile del Servizio gestione documentale, segreteria organi e transizione digitale;

B. l'accesso può essere autorizzato esclusivamente ai referenti informatici dell'Ente;

C. il referente informatico dell'Ente è designato incaricato del trattamento di dati personali che sia strettamente necessario effettuare al fine di adempiere ai compiti assegnatigli con l'istanza di cui alla lettera A);

D. il Responsabile del Servizio gestione documentale, segreteria organi e transizione digitale dispone che uno degli amministratori di sistema attivi la funzione di delega sulla casella di posta o sul cloud, o sulle risorse di rete dell'utente assente, a favore del referente informatico individuato;

E. è fatto divieto al referente informatico di accedere ai messaggi di posta elettronica o file/cartelle che, già dall'oggetto, possano far prefigurare un contenuto riconducibile a informazioni personali non relative all'attività lavorativa del soggetto assente;

F. la funzione di delega descritta rimane attiva per il tempo strettamente necessario al recupero dei contenuti che si reputano indispensabili per dare continuità all'attività

lavorativa oppure per un periodo di tempo predeterminato (quale ad esempio quello della malattia dell'utente assente) al termine del quale la funzione viene automaticamente disattivata:

G. al termine della procedura di accesso e dopo aver trasmesso al Responsabile di Struttura istante i contenuti richiesti, il referente informatico di Struttura redige apposito verbale delle operazioni effettuate che consegnerà agli atti della struttura affinché anche l'utente stesso possa prenderne visione al rientro.

13.4 Reindirizzamento posta elettronica in caso di cessazione del rapporto di lavoro

Nei casi in cui l'utente cessi il proprio rapporto di lavoro con l'Ente, è concessa allo stesso la facoltà di reindirizzare per un periodo di tempo massimo di 30 giorni, i messaggi di posta elettronica ricevuti sulla casella di posta elettronica assegnata dall'Ente verso altro indirizzo email, previa autorizzazione del Responsabile della struttura di appartenenza. L'utente è tenuto ad indicare l'indirizzo di posta elettronica cui reindirizzare i messaggi di posta ricevuti. Al fine di attivare questa funzione, l'utente deve effettuare istanza scritta al responsabile del Servizio gestione documentale, segreteria organi e transizione digitale.

13.5 Autorizzazione all'utilizzo della casella di posta elettronica ad altri collaboratori

Nel caso in cui un utente reputasse opportuno, al fine di organizzare in maniera più efficiente la propria attività lavorativa, autorizzare ulteriori collaboratori (esempio gli addetti alla Segreteria) all'utilizzo della propria casella di posta elettronica, calendario, attività, note, e contatti può utilizzare le funzioni di delega previste dall'applicativo di posta elettronica.

14. CONTROLLI E SANZIONI

14.1 Controlli

La struttura competente in materia di ICT dell'Ente o altri soggetti delegati dal Titolare hanno facoltà di effettuare controlli, anche preventivi, sul corretto uso e funzionamento degli strumenti informatici nel rispetto dei diritti e delle libertà fondamentali dei lavoratori o dei soggetti esterni che utilizzano strumenti informatici dell'Ente al fine di evitare usi impropri dei sistemi messi a disposizione dall'Ente.

Possono essere effettuati controlli automatizzati sul traffico di rete volti a inibire l'accesso a siti o categorie di siti di palese natura non istituzionale.

I controlli sulle attività svolte mediante utilizzo dei sistemi informatici sono ammessi nei seguenti casi:

A. quando previsti da fonte normativa o regolamentare;

B. nel caso in cui si verifichino eventi dannosi o situazioni di pericolo non impediti da preventivi accorgimenti tecnici, per esempio nel caso di attacchi informatici, data breach, ecc.;

C. su segnalazione dell'Autorità Giudiziaria;

D. nel caso in cui, nell'ambito delle ordinarie attività di gestione dei sistemi informativi di competenza, siano rilevati file illegali o dal contenuto palesemente non istituzionale;

E. nell'ambito di controlli saltuari a campione per le finalità di prevenzione data breach.

Nei casi in cui, a seguito di un controllo, si rilevino comportamenti illegali o non istituzionali, la struttura competente in materia di ICT dell'Ente o altri soggetti delegati dal Titolare potranno intervenire valutando se:

- applicare gli strumenti e. procedimenti previsti nel documento data breach (determina n. 176 del 26 luglio 2023)
- inviare avvisi collettivi o individuali in cui verranno segnalati i comportamenti non corretti;
- rimuovere i file, senza alcun preavviso all'utente, nei casi in cui i file possano limitare l'utilizzo di risorse o possano recar danno all'Ente;
- inibire l'accesso a siti o categorie di siti di palese natura non istituzionale;
- informare, nei casi in cui i comportamenti non corretti si ripetano nel tempo o risultino particolarmente gravi, il legale rappresentante o il dirigente del personale, per i rispettivi ambiti di competenza, che adotteranno i provvedimenti più opportuni di cui al paragrafo successivo "sanzioni".

14.2 Sanzioni

I comportamenti in violazione della normativa vigente e del presente disciplinare che hanno una rilevanza disciplinare, fermi restando i diversi profili di responsabilità civile e penale, saranno sanzionati secondo le forme e le modalità previste dai rispettivi ordinamenti degli utenti interessati.

Tali comportamenti sono segnalati al legale rappresentante o al dirigente del personale che valuteranno le modalità di intervento più idonee, anche a tutela di eventuali danni economici e/o di immagine subiti dall'Ente.

15. DECALOGO SINTETICO

1. Non installare programmi diversi da quelli autorizzati e predisposti dall'Azienda.
2. Salvare i dati sul server aziendale, non sul disco del proprio PC.
3. Non utilizzare il computer aziendale per attività personali o extra lavorative.
4. Bloccare il proprio computer ogni qualvolta ci si assenta dall'ufficio.
5. Utilizzare e consultare solo la casella email aziendale.
6. Non consultare email, né scaricare allegati dalla propria posta personale.
7. Impostare password forti ed univoche.
8. Non comunicare le proprie password ad altri.
9. Gli username e le password aziendali non devono in alcun modo essere riutilizzate per servizi Internet estranei all'Azienda.
10. Non utilizzare la rete internet aziendale per navigare in siti non pertinenti all'attività lavorativa.

16. GLOSSARIO

Termine/Acronimo	Descrizione
Analisi forense	insieme di tecniche rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova.
Autenticazione	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'utente che accede ai sistemi informativi.
Black List di Reputation	Insieme di indirizzi (IP, mail) ai quali, sulla base dei comportamenti tenuti precedentemente (es. invio di spam), è impedito l'utilizzo di alcuni servizi informatici.
Cracking (strumenti di)	software che consentono l'aggiramento illecito delle misure di sicurezza di un sistema informatico.

Termine/Acronimo	Descrizione
Data Breach	Vedi definizione in Detetermina n. 176 del 26 luglio 2023 - Data Breach
Dati personali	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati di particolari categorie	dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
Identificazione informatica	la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.
Dispositivo mobile	sistema di elaborazione che può essere spostato e trasportato. Nel contesto del presente disciplinare tecnico, per dispositivo mobile si intende solo “smartphone” o “tablet”, mentre negli altri casi si parla esplicitamente di “computer portatile”, o “postazione di lavoro portatile”
Evidenza	nell’ambito dell’analisi forense, si intende una “traccia” di reato; la raccolta delle evidenze rappresenta una fase della gestione degli incidenti di sicurezza informatica, anche quando non siano presenti implicazioni legali.
Incaricato	la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

Termine/Acronimo	Descrizione
Password	sequenza di caratteri alfanumerici che costituisce la chiave d'accesso ad un sistema protetto. In assenza di altri dispositivi, la password costituisce il meccanismo di sicurezza base per la protezione dell'accesso a risorse informatiche.
Patch	aggiornamento di un software per la correzione di un problema di sicurezza o di funzionalità.
Peer-to-peer (strumenti)	software che permettono l'utilizzo di una postazione di lavoro in modalità server per consentire lo scambio di file con altri utenti, anche esterni alla rete dell'Ente.
Phishing	tecnica finalizzata all'acquisizione, per scopi illegali, di dati riservati (codici di accesso, password, numeri carte di credito e altre informazioni personali) tramite l'invio di e-mail dal contenuto e dal mittente opportunamente falsificati (per es. simulando la provenienza del messaggio da parte di una banca o di uno studio legale).
Postazione di lavoro	Il pc o il portatile comprensivo di tutte le periferiche di input e output (mouse, tastiera, webcam, video, stampante collegata) che costituiscono la dotazione hardware assegnata ad un utente
Ransomware	tipo di malware che limita l'accesso del dispositivo che infetta (per esempio cifrando i dati), richiedendo un riscatto (*ransom* in Inglese) da pagare per rimuovere la limitazione
Responsabile del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Scanning	attività di raccolta di informazioni su un sistema propedeutica alla fase di attacco informatico vero e proprio.
Sniffing (strumenti di)	software che consentono di intercettare ed analizzare il traffico in transito su una rete informatica.

Termine/Acronimo	Descrizione
Spamming	l'invio di grandi quantità di messaggi elettronici non richiesti (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.
Spyware	software che raccoglie informazioni riguardanti un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata.
Supporto rimovibile	dispositivo su cui è possibile registrare dati che può essere facilmente rimosso dal sistema che lo legge/scrive, trasportato in altri luoghi e collegato ad altri sistemi. Esempi di supporti rimovibili sono: chiavette USB, hard disk esterni, CD ROM.
Titolare del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri
Worm	programma in grado di autodiffondersi sulla rete e verso altri sistemi.
Virus	programma in grado di autoreplicarsi in un sistema, per esempio copiando una parte di se stesso all'interno del codice di un altro programma.