# COMUNE DI USSASSAI

**PROV. OGLIASTRA**

Via Nazionale, 120 - CAP 08040 - USSASSAI

CF/P. IVA 00160240917 - TEL. 0782 55710 – FAX 0782 55890


# PIANO DI SICUREZZA

## (art. 4, comma 1, lett.c), DPCM 3 dicembre 2013)

### PARTE I – DISPOSIZIONI GENERALI

#### 1.0.AMBITO DI APPLICAZIONE

Il presente Piano di Sicurezza viene adottato ai sensi dell'articoli 4, 1° comma lettera c), e 5 del DPCM 3 dicembre 2013, in materia di "*Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*".

Così come disposto dal summenzionato art. 4, 1° comma lettera c), DPCM 3 dicembre 2013, il Responsabile della gestione documentale ha il compito di "*predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi o, nel caso delle pubbliche amministrazioni centrali, il responsabile dell'ufficio di cui all'art. 17 del Codice e con il responsabile del trattamento dei dati personali di cui al suddetto decreto*".

Il Piano di Sicurezza è redatto dal Comune di Ussassai, corrente in Ussassai (OG), alla Via Nazionale n.° 120. Per maggiori dettagli si rimanda alla tabella riepilogativa contenuta in calce al presente documento.

Il Piano di Sicurezza redatto dal Comune di Ussassai, garantisce che i documenti e le informazioni trattati dall'Ente siano resi disponibili, integri e riservati e che i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

### 1.1.REQUISITI MINIMI DI SICUREZZA

L'art. 7 del DPCM 3 dicembre 2013, indica i requisiti minimi di sicurezza del sistema di protocollo informatico, al quale il presente Piano si conforma, prevedendo come il sistema di cui sopra debba assicurare:

a) l'univoca identificazione ed autenticazione degli utenti;
b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Inoltre, il sistema di protocollo informatico deve consentire:

- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;
- il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Infine, il sistema di protocollo rispetta le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

### 1.2.IL SISTEMA DI GESTIONE INFORMATICA DOCUMENTALE – IL PROTOCOLLO INFORMATICO

Nel rispetto di quanto disposto dall'art. 7 del DPCM 3 dicembre 2013 e tenuto conto di quanto statuito dall'art. 61, 3° comma, DPR 445/2000 l'Ente, nell'istituzione del servizio per la tenuta del protocollo informatico, nella gestione dei flussi documentali e degli archivi nell'ambito dell'AOO, dovrà fare in modo che tale servizio:

1. attribuisca il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
2. garantisca che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del DPR 445/2000;
3. garantisca la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53 del DPR 445/2000 e dell'articolo 7, 5° comma, del DPCM 3 dicembre 2013;
4. curi che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;

5. conservi le copie di cui agli articoli 62 e 63 del DPR 445/2000, in luoghi sicuri;
6. garantisca il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 del DPR 445/2000 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69 del medesimo TU;
7. autorizzi le operazioni di annullamento di cui all'articolo 54 del DPR 445/2000;
8. vigili sull'osservanza delle disposizioni del DPR 445/2000 da parte del personale autorizzato e degli incaricati.

Pertanto, l'Ente ha provveduto ad adottare le necessarie misure tecniche ed organizzative al fine di assicurare la sicurezza tecnologica dell'AOO, la riservatezza dei dati e delle informazioni e l'univoca identificazione degli utenti, attraverso i seguenti accorgimenti:

- protezione della rete informatica dell'Ente attraverso l'attivazione di un *firewall* perimetrale e la configurazione dei *firewall* locali di sistema su tutti gli elaboratori;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (*user ID*), di una credenziale riservata di autenticazione (*password*);
- esecuzione e gestione delle copie di *backup* dei dati e dei documenti da effettuarsi con frequenza giornaliera;
- ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio del software di gestione documentale;
- invio al sistema di conservazione del registro giornaliero di protocollo, da effettuare entro la giornata lavorativa successiva a quella della sua produzione, garantendone l'immodificabilità del contenuto;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei *file* di *log* di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema;
- impiego e manutenzione di un adeguato sistema *antivirus* e di gestione dei rispettivi aggiornamenti, correttivi dei sistemi operativi.

I dati personali registrati nel *log* del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il Sistema di Gestione Informatica dei Documenti (Protocollo Informatico)

saranno consultati solo in caso di necessità da soggetti autorizzati in virtù di specifiche norme di legge.

## 1.3.AGGIORNAMENTO E PUBBLICAZIONE DEL PIANO DI SICUREZZA

Il Piano di Sicurezza dell'Ente è soggetto a revisione con cadenza almeno biennale.

Ad ogni modo, a seguito di particolari esigenze determinate da sopravvenienze normative ovvero da evoluzioni tecnologiche, potrà essere modificato anticipatamente.

Il Piano di Sicurezza, essendo parte integrante del Manuale di Gestione (*ex* articolo 5, 2° comma, lettera b) del DPCM 3 dicembre 2013) dovrà essere pubblicato, così come previsto dall'articolo 5, 3° comma, DPCM 3 dicembre 2013, nel sito istituzionale dell'Ente all'indirizzo www.comune.ussassai.og.it

## PARTE II – ELEMENTI DI RISCHIO

### 2.0.ANALISI DEI RISCHI

L'Ente ha stabilito come i principali elementi di rischio, cui sono sottoposti i documenti ed i dati trattatati per il tramite del Sistema di Gestione Informatica dei Documenti, sono sostanzialmente riportabili alla cancellazione o manomissione dei documenti e dei dati, includendo a tale proposito tutti i dati presenti sul Sistema di Gestione Informatica dei Documenti.

Per prevenire tale rischio e le conseguenze da esso derivanti, nonché altri che potrebbero concretizzarsi, l'Ente adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

### 2.1.ACCESSO ALLA RETE INFORMATICA DELL'ENTE

È presente un *firewall* perimetrale, che protegge tutta la rete informatica dell'Ente, sono poi stati configurati i *firewall* locali di sistema su tutti gli elaboratori.

Inoltre, il Sistema di Gestione Informatica dei Documenti dell'Ente non è esposto all'accesso attraverso la rete Internet, ma opera all'interno di uno dei server installato nella rete LAN dell'Ente, usufruendo dalla stessa tutti i meccanismi previsti per la sicurezza e la protezione.

### 2.2.ACCESSO AL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

In merito all'accesso al Sistema di Gestione Informatica dei Documenti, lo stesso si realizza attraverso l'utilizzo di credenziali di autenticazione.

Ad ogni utente del sistema di gestione del protocollo e dei documenti, viene assegnata una credenziale di identificazione pubblica (*user ID*) ed una credenziale riservata di autenticazione (*password*), al fine di superare una procedura di autenticazione che consente l'accesso ai soli operatori abilitati e che tiene traccia di tutti gli accessi di ciascun utente.

Tale misura prevede la creazione di una *password*, di almeno otto caratteri, la quale non dovrà contenere nessun riferimento facilmente ricollegabile all'organizzazione, all'utilizzatore o all'Ente.

La stessa dovrà essere modificata ogni sei o tre mesi, a seconda che siano trattati, rispettivamente, dati comuni o sensibili/giudiziari in formato elettronico.

Agli utenti del sistema di gestione del protocollo e dei documenti, è stato prescritto di adottare le necessarie cautele per assicurare la segretezza della *password*.

Gli Incaricati scelgono autonomamente la *password* e provvedono alla sua custodia in busta chiusa che, successivamente, viene consegnata al custode delle *password*.

Quest'ultimo è stato nominato, con apposita lettera, e, oltre ad essere il responsabile della gestione delle credenziali di autenticazione, nel rispetto di quanto previsto dalla normativa, provvede anche alla custodia delle buste in un luogo sicuro.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate.

Ciò si verifica altresì nell'ipotesi in cui si realizzi la perdita della qualità che consente all'Incaricato l'accesso ai dati personali.

Tale disattivazione potrà avvenire con l'ausilio del personale tecnico esterno al quale l'Ente si rivolge.

Non è prevista, allo scadere dei sei mesi, la disattivazione delle credenziali preventivamente autorizzate unicamente per scopi di gestione tecnica

L'Ente ha provveduto ad impartire specifiche istruzioni agli incaricati affinché non venga lasciato incustodito e accessibile l'elaboratore durante una sessione di trattamento.

Inoltre, in caso di prolungata assenza o impedimento dell'Incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, è prevista l'apertura della busta contenente la password, previa comunicazione di ciò all'Incaricato interessato, il quale provvederà, una volta rientrato in servizio, alla modifica della password di cui sopra.

Per quanto invece attiene l'accesso ai documenti ed ai dati contenuti nel Sistema di Gestione Informatica dei Documenti da parte degli incaricati facenti parte dell'AOO, sono stati individuati diversi profili di autorizzazione, pertanto, si è utilizzato un sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato, o per classi omogenee di incaricati, sono stati individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento medesimo.

I profili di autorizzazione sono stati creati tenendo conto del livello di sicurezza di ciascun documento, fascicolo, sottofascicolo, ecc.

Periodicamente e comunque con cadenza almeno annuale, viene verificata la sussistenza dei requisiti e delle condizioni per la conservazione dei profili di autorizzazione.

Il Sistema di Gestione Informatica dei Documenti consente di associare differenti livelli di riservatezza per ogni tipo di documento trattato dall'AOO

Tali livelli si distinguono in abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione ed alla modifica delle informazioni.

I documenti non sono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nel Sistema medesimo.

### 2.3.ACCESSO DI UTENTI ESTERNI AL SISTEMA

L'accesso al Sistema di Gestione Informatica dei Documenti dell'Ente d parte di altre AOO della PA avviene nel rispetto dei principi di interoperabilità e della cooperazione applicativa. L'accesso al

Sistema di Gestione Documentale – Protocollo/AOO, è consentito esclusivamente dalla rete LAN dell'Ente.

Gli utenti privati esterni all'Ente non possono accedere ai documenti direttamente per via telematica attraverso una apposita procedura di autenticazione e riconoscimento a seguito dell'inserimento di un identificativo univo (*user ID*) e di una *password*, ovvero attraverso apposita *smart card*.

L'esercizio del diritto di accesso da parte di utenti privati esterni al Sistema viene garantito nel rispetto di quanto statuito dalla L.241/1990, dal D.Lgs. 196/2003 e dal D.Lgs. 33/2013.

## 2.4.TRATTAMENTO DEI DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Così come disposto dagli articoli 27, 28 e 29 dell'Allegato B – Disciplinare tecnico in materia di misure minime di sicurezza – al D.Lgs.196/2003:

- agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione (art. 27 Allegato B);
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate (art. 28 Allegato B);
- l'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate (art. 29 Allegato B).

## PARTE III – LA FORMAZIONE DEI DOCUMENTI

### 3.0.FORMATI E SOTTOSCRIZIONE DEI DOCUMENTI DIGITALI

I documenti digitali gestiti nell'ambito dell'AOO, sono prodotti utilizzando i formati previsti dall'Allegato 2 del DPCM 3 dicembre 2013.

Prima della sottoscrizione del documento digitale da parte degli incaricati facenti parte dell'AOO, questi provvedono alla sua conversione in uno dei formati di cui sopra.

Tale conversione avviene preferibilmente nel formato PDF e P7M.

Con la sottoscrizione del documento digitale tramite firma digitale, viene garantita:

- l'attribuzione certa della titolarità del documento;
- l'integrità del documento.

Pertanto, attraverso le risorse strumentali a disposizione dell'Ente e le procedure utilizzate per la formazione dei documenti digitali si andrà a garantire:

- l'identificabilità del soggetto che ha formato il documento digitale nonché l'Ufficio dell'Ente ovvero l'AOO di riferimento;
- la sottoscrizione del documento digitale;
- l'idoneità del documento digitale ad essere gestito tramite strumenti informatici e ad essere registrato nel Sistema di Gestione Informatica dei Documenti;
- l'accesso al documento digitale tramite sistemi informativi automatizzati;
- la leggibilità del documento digitale nel tempo;
- l'interscambiabilità del documento digitale all'interno dell'Ente.

La sottoscrizione del documento digitale avverrà prima della sua registrazione nel Sistema di Gestione Informatica dei Documenti.

### 3.1.REGISTRAZIONI DI PROTOCOLLO

Le registrazioni, nonché l'effettuazione delle eventuali modifiche al protocollo informatico, possono essere effettuate unicamente dal personale abilitato, così come l'accesso in consultazione.

Ogni registrazione di protocollo viene memorizzata dal Sistema di Gestione Informatica dei Documenti, unitamente all'identificativo univoco (alle generalità) dell'autore che l'ha eseguita.

Qualora siano autorizzate delle modifiche a precedenti registrazioni di protocollo, tali modifiche vengono registrate per mezzo di *log* di sistema che mantengano traccia dell'autore, della modifica effettuata, nonché della data e dell'ora.

Inoltre, nell'ipotesi di modifiche a precedenti registrazioni, il Sistema mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione.

Il Sistema di Gestione Informatica dei Documenti non permette la modifica del numero e della data di protocollo.

Qualora si rendesse necessaria una simile modifica si potrà unicamente provvedere all'annullamento della registrazione stessa di cui, analogamente al caso precedente, il Sistema manterrà traccia.

Nell'ipotesi in cui si provveda all'annullamento di una registrazione di protocollo, questa sarà accompagnata da un'autorizzazione scritta del Responsabile della gestione documentale, inoltre il Sistema di Gestione Informatica dei Documenti indicherà, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione.

Il Sistema di Gestione Informatica dei Documenti, al fine di garantire l'immodificabilità delle registrazioni di protocollo, prevede, a conclusione della giornata lavorativa, a produrre il registro giornaliero delle registrazioni di protocollo in formato digitale.

L'Ente, nel rispetto di quanto previsto dall'art. 7, 5° comma, DPCM 3 dicembre 2013, provvede a trasmettere il registro giornaliero di protocollo, entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

## PARTE IV – GESTIONE DEI DOCUMENTI INFORMATICI

### 4.0.GESTIONE DEI DOCUMENTI DIGITALI E SICUREZZA

Così come disposto dal DPCM 13 novembre 2014 in materia di documenti informatici, con la registrazione di questi ultimi in un sistema di gestione documentale che adotti idonee politiche di sicurezza, vengono garantite le caratteristiche di immodificabilità e di integrità del documento stesso (art. 3, 4° comma, DPCM 13 novembre 2014).

L'acceso ai documenti digitali che sono stati registrati nel Sistema di Gestione Informatica dei Documenti, potrà avvenire da parte degli incaricati attraverso la loro autenticazione al Sistema stesso, tramite l'inserimento delle credenziali di autenticazione personali e nel rispetto dei differenti profili di autorizzazione creati per ciascun utente.

Unicamente gli incaricati, abilitati per lo svolgimento delle diverse attività, possono effettuare operazioni sul Sistema di Gestione Informatica dei Documenti o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti.

Come sopra evidenziato, il Sistema di Gestione Informatica dei Documenti tiene traccia di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione, inoltre, tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Tenuto conto di quanto disposto dagli articoli 16 e 20 dell'Allegato B – Disciplinare tecnico in materia di misure minime di sicurezza – al D.Lgs.196/2003, il Sistema di Gestione Informatica dei Documenti, nonché i documenti e dati in esso contenuti, sono protetti contro i rischi di accesso abusivo e contro l'azione di programmi informatici mediante l'attivazione di strumenti quali:

- *firewall* perimetrale, che protegge tutta la rete informatica dell'Ente;
- *firewall* locali di sistema su tutti gli elaboratori;
- dispositivo *antivirus* ed *antispyware* che viene aggiornato con funzione automatica, appena ci si collega ad Internet. Qualora nessun aggiornamento fosse segnalato automaticamente per un periodo di un mese, si provvede ad effettuare un controllo per verificare l'esistenza di detti aggiornamenti automatici. Si effettua anche la scansione periodica di tutti i dati presenti nel sistema informatico.

Affinché sia ridotto il rischio di vulnerabilità al sistema informatico dell'Ente, è altresì previsto l'aggiornamento periodico del sistema operativo in uso presso l'AOO nonché l'adeguamento dell'applicativo del Sistema di Gestione Informatica dei Documenti (Protocollo Informatico).

Tali aggiornamenti avvengono in automatico, tramite connessione ad Internet, ovvero tramite gli aggiornamenti forniti dall'azienda che offre assistenza ai software medesimi.

### 4.1.SALVATAGGIO E RIPRISTINO DEI DATI

Così come disposto dall'articolo 18 dell'Allegato B – Disciplinare tecnico in materia di misure minime di sicurezza – al D.Lgs.196/2003, si provvede periodicamente all'effettuazione del salvataggio dei dati contenuti nel Sistema di Gestione Informatica dei Documenti.

Il backup di tali dati avviene con cadenza giornaliera.

Tale procedura è posta in essere automaticamente.

Le copie vengono effettuate su dispositivo NAS (Network Attached Storage), che è posizionato in una stanza chiusa al piano terra dell'edificio.

In merito al ripristino del sistema informativo, è stato previsto come lo stesso venga effettuato entro sette giorni in caso di disastro, come statuito dall'articolo 23 del summenzionato Allegato B.

## PARTE V – TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI

### 5.0.TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

La trasmissione e l'interscambio dei documenti e dei fascicoli informatici all'interno dell'Ente avviene per il tramite del Sistema di Gestione Informatica dei Documenti, al fine di evitare la dispersione e la circolazione incontrollata dei documenti e dei dati (ovvero avviene anche tramite Posta elettronica ordinaria/certificata ed un'apposita cartella condivisa).

La trasmissione dei documenti informatici all'esterno dell'Ente avviene tramite PEC o mediante i sistemi di interoperabilità e di cooperazione applicativa di cui al Sistema Pubblico di Connettività, utilizzando le informazioni contenute nella segnatura di protocollo.

In merito ai messaggi di posta elettronica, l'articolo 5.8 dell'Allegato 2 al DPCM 3 dicembre 2013, prevede come ai fini della loro conservazione, lo standard a cui fare riferimento, per preservarne l'autenticità, è RFC 2822/MIME, mentre per quanto riguarda il formato degli allegati al suddetto messaggio si utilizzeranno, a seconda della tipologia del documento trattato e delle esigenze, i formati elettronici precedentemente indicati dal medesimo Allegato 2.

### 5.1.TUTELA DELLA RISERVATEZZA

I dati, i documenti, i certificati, ecc., che sono oggetto di trasmissione e di interscambio all'interno della AOO ovvero ad altre PA, al fine della tutela della riservatezza dei dati personali in essi contenuti, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è permesso il trattamento e che sono strettamente necessarie per il perseguimento delle finalità per le quali è stata prevista la trasmissione ed l'interscambio.

## PARTE VI – CONSERVAZIONE DEI DOCUMENTI INFORMATICI

### 6.0.CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La conservazione dei documenti informatici deve avvenire nel rispetto delle regole tecniche contenute nel DPCM 3 dicembre 2013.

L'Amministrazione provvede alla conservazione documentale per quanto attiene il registro giornaliero di protocollo, affidando il servizio di conservazione ad un conservatore accreditato esterno (CREDEMTEL).

## PARTE VII – STRATEGIE DI SICUREZZA

### 7.0.STRATEGIE DI SICUREZZA ADOTTATE DALL'ENTE

L'utente fruitore del Sistema di Gestione Informatica Documentale è responsabile delle azioni poste in essere durante l'utilizzo del Sistema stesso.

Qualora si dovesse procedere alla registrazione di un nuovo utente autorizzato alla fruizione del Sistema, si procede attraverso un'apposita procedura con la quale sono annotate le necessarie informazioni riportabili all'utente ed al suo ruolo di appartenenza.

Le credenziali per l'accesso al Sistema non devono essere cedute ovvero comunicate a terzi per nessuna ragione.

La responsabilità delle operazioni poste in essere tramite una specifica utenza sono riconducibili unicamente al titolare della stessa, anche se compite in sua assenza, a meno che non si sia dovuto intervenire per ragioni di sicurezza e di tale intervento sia data rilevanza per iscritto, fermo restando che l'utente dovrà, una volta tornato in servizio, provvedere alla modifica delle proprie credenziali di autenticazione.

### 7.1.POSTAZIONI DI LAVORO

Al fine di evitare perdite, compromissioni, diffusioni non autorizzate, ecc., dei dati, tutelandone al contempo l'accesso, l'incaricato del Sistema di Gestione Informatica dei Documenti, nella gestione del proprio posto di lavoro:

- non dovrà mai lasciare incustodita la propria postazione di lavoro, neanche per brevi periodo, qualora sia attiva una sessione di lavoro;
- qualora si allontani dalla propria postazione di lavoro, anche momentaneamente, dovrà attivare i necessari strumenti di protezione affinché non sia consentito a persone non autorizzate di prendere visione della sessione di lavoro intrapresa (ad esempio attraverso la predisposizione dello screensaver con password o del blocco del terminale attraverso la procedura del CTRL – ALT – CANC);
- dovrà tenere la propria postazione in ordine, non lasciando materiale riservato incustodito al di fuori delle necessarie sessioni di trattamento e comunque non oltre l'orario di lavoro, provvedendo a conservare il materiale di lavoro negli appositi armadi dotati di serratura, premunendosi di chiudere gli stessi a chiave e di asportare queste ultime, di disattivare o bloccare il terminale e di tenere chiusi i locali dove avvengono i trattamenti dei dati, al fine di evitare l'accesso di personale non autorizzato.

## TABELLA RIEPILOGATIVA

| | |
|---|---|
| DENOMINAZIONE AMMINISTRAZIONE | Comune di Ussassai |
| INDIRIZZO SEDE LEGALE AMMINISTRAZIONE (via, CAP, città, provincia) | Via Nazionale n.° 120 – 08040 Ussassai (OG) |
| REGIONE SEDE LEGALE AMMINISTRAZIONE | Sardegna |
| INDIRIZZO PEC | protocollo@pec.comune.ussassai.og.it |
| INDIRIZZO POSTA ELETTRONICA ORDINARIA | sindaco@comune.ussassai.og.it |
| INDIRIZZO SITO ISTITUZIONALE | www.comune.ussassai.og.it |
| NOMINATIVO LEGALE RAPPRESENTATE | Gian Basilio Deplano |
| INDICAZIONE AOO | Area Amministrativa |
| INDIRIZZO PEC AOO | protocollo@pec.comune.ussassai.og.it |
| NOMINATIVO RESPONSABILE GESTIONE DOCUMENTALE | Gian Basilio Deplano |
| NOMINATIVO VICARIO DEL RESPONSABILE GESTIONE DOCUMENTALE | Roberta Guaraldo<br>Lisa Mura<br>Mauro Serrau |