# Comune di Burcei
**(Provincia di Cagliari)**

# Documento Programmatico sulla Sicurezza
(ai sensi del D.Lgs. n.196/2003)

## 1. SCOPO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Questo Documento Programmatico sulla Sicurezza (d'ora in poi "D.P.S.") è adottato, ai sensi del D.Lgs. n.196/2003 per definire le politiche di sicurezza in materia di trattamento di dati informatici e di accesso a banche dati sensibili e personali, insieme ai criteri organizzativi per la loro attuazione.
In particolare, in questo D.P.S. e nei suoi allegati A – Analisi situazione, B – Disciplinare tecnico, C – Nomina dei soggetti preposti, sono definiti i criteri tecnici e organizzativi per:

- la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
- i criteri e le procedure per assicurare l'integrità dei dati;
- i criteri e le procedure per la sicurezza della trasmissione dei dati, compresi quelli per le redazioni di accesso per via telematica;
- l'elaborazione di un piano di formazione per informare gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

## 2. CAMPO DI APPLICAZIONE

Il D.P.S. definisce le politiche e gli standard di sicurezza, in merito al trattamento dei dati informatici, alla loro sicurezza e alla tutela della privacy sui dati personali; è realizzato nel rispetto di quanto indicato nel Disciplinare Tecnico di attuazione delle norme sulla sicurezza dei dati informatici e sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, adottato dal Comune (Allegato B al Dlgs n.196/2003, d'ora in poi "Disciplinare Tecnico").
Il D.P.S. riguarda tutti i dati personali detenuti e trattati dal Comune per i propri fini istituzionali e concernenti informazioni di tipo:

- Personale
- Sensibile
- Giudiziario

Il D.P.S. si applica al trattamento di tutti i dati per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, etc.)

Il D.P.S. deve essere conosciuto ed applicato da tutti gli uffici del Comune.

## 3. RIFERIMENTI NORMATIVI

Questo D.P.S. trae conforto normativo dalle leggi e norme statali meglio esplicitate nel Disciplinare Tecnico a cui si fa riferimento per ogni dettaglio.

## 4. NOMINA DELLE SINGOLE FIGURE PREVISTE DALLA NORMATIVA A PROTEZIONE DEI DATI PERSONALI NEL SETTORE DELLA SICUREZZA

### 4.1 - NOMINA DEL TITOLARE DEL TRATTAMENTO DEI DATI

Assume il ruolo di Titolare del trattamento dei dati il legale rappresentante del Comune, nella persona del sindaco

_____

### 4.2 - NOMINA DEL RESPONSABILE DELLA SICUREZZA E DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento dei dati nomina Responsabile della sicurezza e del trattamento dei dati, a far data dal _____, :

_____

Questa nomina è regolarmente deliberata con il provvedimento della Giunta Comunale che costituisce l'allegato C a questo D.P.S.
Il Titolare del trattamento dei dati deve informare il Responsabile della sicurezza e del trattamento dei dati, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore.
Al Responsabile della sicurezza e del trattamento dei dati il Titolare del trattamento deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Responsabile della sicurezza e del trattamento dei dati: è a tempo indeterminato e decade per revoca o dimissioni dello stesso; può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso ed eventualmente affidata ad altro soggetto.

4.3 - NOMINA DEI RESPONSABILI DI SETTORE DEL TRATTAMENTO DEI DATI
La Giunta Comunale NON ritiene opportuno effettuare la nomina di ulteriori Responsabili di settore del trattamento dei dati.

4.4 - NOMINA DEL CUSTODE DELLE PASSWORD
Il Titolare del trattamento dei dati nomina, a far data dal _____, in qualità di Custode delle Password:

_____

La nomina del Custode delle password deve essere effettuata con una lettera di incarico, controfirmata dall'interessato per accettazione. Copia della lettera di nomina accettata deve essere conservata a cura dell'Amministratore di sistema in luogo sicuro.
Il Titolare del trattamento dei dati deve informare il Custode delle password della responsabilità che gli è stata affidata in relazione a quanto disposto dalle normative in vigore.
Al Custode delle password il Titolare del trattamento deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del Custode delle password: è a tempo indeterminato e decade per revoca o dimissioni dello stesso; può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati ed essere affidata ad altro soggetto.

4.5 - NOMINA DELL'AMMINISTRATORE DI SISTEMA
Il Titolare del trattamento dei dati nomina, a far data dal _____, in qualità di Amministratore di Sistema:

_____

L'Amministratore di sistema sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di banche dati.
Il Titolare del trattamento dei dati può nominare ulteriori Amministratori di sistema, specificando gli elaboratori o le banche dati che sono chiamati a sovrintendere, informandoli delle responsabilità che sono state loro affidate in relazione a quanto disposto dalle normative in vigore.
La lettera di incarico deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del Titolare del trattamento dei dati in luogo sicuro.
All'Amministratore di sistema il Titolare del trattamento deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

4.6 - NOMINA DEGLI INCARICATI DEL TRATTAMENTO DEI DATI
Al Responsabile della sicurezza e del trattamento dei dati è affidato il compito di nominare, con comunicazione scritta, uno o più Incaricati del trattamento dei dati.
La nomina di ciascun Incaricato del trattamento dei dati deve essere effettuata con una lettera di incarico in cui sono specificati i compiti che gli sono affidati.
Gli Incaricati del trattamento devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.
Agli incaricati deve essere assegnata una parola chiave ed un codice identificativo personale.
La nomina degli Incaricati del trattamento deve essere controfirmata dall'interessato per presa visione e copia della stessa e deve essere conservata a cura del Responsabile del trattamento per la sicurezza dei dati in luogo sicuro.
Agli Incaricati del trattamento, il Responsabile della sicurezza e del trattamento dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina degli Incaricati è a tempo indeterminato e decade per revoca, per sue dimissioni, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

Sono nominati i soggetti autorizzati al trattamento dei dati sensibili in possesso del Comune per l'esecuzione materiale:

| Cognome e Nome | Settore |
|---|---|
| Anna Maria Pischedda | SEGRETARIO GENERALE |
| Zoncheddu Zelinda | FINANZIARIO |
| Cannas Ignazia | FINANZIARIO |
| Pusceddu Franco | TRIBUTI |
| Zuncheddu Rita | SERVIZI DEMOGRAFICI |
| Tolu Angela Maria | SERVIZI DEMOGRAFICI |
| Zuncheddu Rita | A.VA POLIZIA MUNICIPALE |
| Vacca Antonello | A.VA POLIZIA MUNICIPALE |
| Corda Antonio | TECNICA |
| Serra Dino | TECNICA |
| Serreli Innocenzo | TECNICA |
| Monni Rosetta | AFFARI GENERALI |
| Marcia Maria Carmela | AFFARI GENERALI |
| Salvatore Staffa | SERVIZI SOCIALI |

Queste nomine sono regolarmente convalidate dagli organismi competenti che hanno Titolarità al trattamento dei dati con i provvedimenti dell'Amministrazione o con le lettere d'incarico controfirmate e che costituiscono allegato a questo D.P.S

## 5. COMPITI DELLE SINGOLE FIGURE PREVISTE DALLA NORMATIVA A PROTEZIONE DEI DATI PERSONALI NEL SETTORE DELLA SICUREZZA.

5.1 - COMPITI DEL TITOLARE DEL TRATTAMENTO DEI DATI

E' onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurino e garantiscano che siano adottate le misure di sicurezza, ai sensi del D.Lgs. n.196/2003.

Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto.

5.2 - COMPITI DEL RESPONSABILE DELLA SICUREZZA E DEL TRATTAMENTO DEI DATI

Il Responsabile del trattamento dei dati è individuato tra i soggetti che per esperienza, capacità e affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo relativo alla sicurezza.

Il Responsabile della sicurezza e del trattamento dei dati dovrà essere una figura preferibilmente di profilo apicale, comunque interna e facente parte a pieno titolo dell'organigramma d'impiego giuridico del personale del Comune. A questa titolarità faranno quindi capo tutti gli obblighi e le responsabilità previsti dalle norme di cui al precedente punto 3 (riferimenti normativi).

In relazione all'attività del Responsabile del trattamento dei dati, è prevista la nomina di uno o più Responsabili di Settore del trattamento dei dati, con compiti diversi a seconda delle funzioni svolte nei diversi settori di attività del Comune.

E' onere del Responsabile del trattamento dei dati adottare le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto ai Responsabili di Settore del trattamento dei dati.

Al Responsabile del trattamento dei dati compete l'autorizzazione, previa comunicazione al Titolare e , nel caso si rendesse necessario, al Garante per la Privacy, del trattamento di nuove banche di dati personali, sensibili o giudiziari.

5.3 COMPITI DEI RESPONSABILI DI SETTORE DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento affida ove le figure siano presenti ai singoli Responsabili di Settore del trattamento dei dati l'onere di individuare, nominare ed indicare per iscritto uno o più funzionari autorizzati con funzioni di Incaricati del trattamento, interni al proprio settore ed autorizzati ad operare sui dati eventualmente detenuti e gestiti.

Ogni Responsabile di Settore del trattamento dei dati ha il compito di:

- attribuire, con l'ausilio degli Amministratori di sistema, ad ogni Utente (USER) o incaricato un Codice identificativo personale (LOGIN-ID) per l'utilizzazione e l'accesso alle banche dati dell'Amministrazione, che deve essere individuale e non riutilizzabile;
- comunicare al custode delle password la relativa attribuzione delle stesse per la definitiva attivazione e per le operazioni di conservazione in busta;
- autorizzare i singoli incaricati del trattamento e della manutenzione, nel caso di trattamento di dati sensibili, se si utilizzano elaboratori accessibili in rete; per gli stessi dati, se il trattamento è effettuato tramite elaboratori accessibili in rete, e/o resi comunque disponibili al pubblico, dovranno considerarsi oggetto di autorizzazione anche gli strumenti hardware e software da utilizzare, che devono pertanto essere dichiarati pienamente compatibili con il sistema e la piattaforma esistente;
- verificare, con l'ausilio dell'Amministratore di sistema, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali e le misure indicate nell'allegato B a questo Documento;
- garantire che tutte le misure di sicurezza riguardanti i dati in possesso del Comune siano applicate all'interno delle proprie strutture ed eventualmente al di fuori della stessa, se sono cedute a soggetti terzi quali Responsabili del trattamento tutte o parte delle attività di trattamento, eventualmente effettuabili anche mediante connessione telematica;
- informare il Responsabile del Trattamento nella eventualità che si siano rilevati dei rischi;
- richiedere l'autorizzazione al Responsabile del Trattamento dei dati, nel caso di istituzione di nuovi trattamenti di dati personali, sensibili o giudiziari.

Ove l'ente non rilevi la necessità di nominare i Responsabili di settore per il trattamento dei dati tali compiti si rifanno al Responsabile della sicurezza e del trattamento dei dati.

5.4 COMPITI DEL CUSTODE DELLE PASSWORD

E' compito del Custode delle password gestire e custodire le password per l'accesso ai dati da parte degli Incaricati.

Il Custode delle password deve predisporre, per ogni Incaricato del trattamento, un modulo sulla quale devono essere indicati gli User-Id e le password a lui destinati e da utilizzare per l'accesso alle banche dati.

All'interno della busta chiusa dovranno essere indicate in chiaro le password da utilizzare, univocamente correlata agli User ID, per accedere alle postazioni e alle banche dati.

E' sempre compito del Custode delle password detenere le buste contenenti la certificazione delle stesse con relativo utente (User-Id) di attribuzione e sovrintendere alla loro regolare conservazione in luogo chiuso e protetto.

Il Custode delle password dovrà inoltre accertarsi, con l'ausilio dell'Amministratore di sistema, della consistenza e persistenza d'uso ed eventualmente provvedere alla revoca di tutte quelle password con relativo annullamento o sospensione degli User-Id non utilizzati per un periodo superiore a 6 (sei) mesi.

5.5 COMPITI DELL'AMMINISTRATORE DI SISTEMA

E' compito dell'Amministratore di sistema:

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di backup;
- assicurarsi della qualità delle copie di backup dei dati e della loro conservazione in luogo adatto e sicuro;
- fare in modo che sia prevista la disattivazione dei Codici identificativi personali (USER-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso

all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali (USER-ID) per oltre 6 mesi;
- proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi;
- redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi alla piattaforma interna o alla rete pubblica;
- provvedere alla redazione (entro il 31 marzo di ogni anno) di un documento denominato "Censimento del Sistema Informativo" contenente una dettagliata elencazione di sistemi elaborativi, postazioni di lavoro, consegnatari e incaricati insieme alla tipologia di dati trattati.

La documentazione del "Censimento del Sistema Informativo", da includersi come parte integrante nell'Analisi della situazione (Allegato A), potrà essere realizzata secondo un modello cartaceo di scheda per ognuna delle postazioni fisiche di lavoro esistenti. Questo modello potrà essere comunque personalizzato, ma dovrà contenere una indicazione obbligata dei seguenti elementi:

- Caratteristiche hardware dell'unità (memorie, dischi, processori, video)
- Sistema Operativo di base e/o utilizzato per la connessione alla rete intranet/internet
- Software di controllo della sicurezza e caratteristiche per l'accesso ai dati residenti localmente o condivisi sulla rete, se esistente (motori RDBMS, antivirus, firewall software ecc.)
- Eventuali periferiche o metodi misti hardware/firmware/software dedicati al controllo degli accessi (password su bios e firmware locali, sistemi di autenticazione con riconoscimento dell'utente, quali sistemi biometrici, smart cards di firma digitale o similari)
- Software Applicativo installato e utilizzato per il trattamento di informazioni locali
- Software Applicativo installato e utilizzato per il trattamento delle informazioni sulla rete
- Periferiche hardware fisicamente connesse alla postazione
- Consegnatario interno responsabile della postazione e area di appartenenza del Comune
- Indirizzo di riferimento sulla rete fisica (n° di borchia fonia/dati, i.p. address o simili)
- Responsabile ai fini del patrimonio, se si tratta di beni soggetti a inventario
- Codice univoco identificativo della scheda di censimento o matricola della postazione, se inventariata

Il "Censimento del Sistema Informativo" potrà anche essere costituito da un archivio informatico sostitutivo dell'allegato cartaceo (purché lo stesso venga memorizzato su supporto digitale non riscrivibile e sia reso visibile in un formato standard non criptato). Questo archivio dovrà essere comunque memorizzato nella sua forma definitiva alla data di creazione del D.P.P.S e alle successive scadenze annue.

## 6. DATI AFFIDATI ALL'ESTERNO PER IL TRATTAMENTO

### 6.1 - TRATTAMENTO DEI DATI IN OUTSOURCING

Il Responsabile della sicurezza e del trattamento dei dati può decidere, in seguito a richiesta da parte del Responsabile di Settore del trattamento dei dati di competenza, di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, in outsourcing, nominandoli Responsabili del trattamento.
In questo caso debbono essere specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.
Nel caso in cui questi non siano espressamente nominati, i Responsabili del trattamento in outsourcing, ai sensi dell'art. 29 del D.Lgs. n. 196/2003, devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.
Il Titolare del trattamento o uno dei Responsabili del trattamento, cui è affidato questo specifico incarico, deve redigere e aggiornare, ad ogni variazione, l'elenco dei soggetti che effettuano il trattamento dei dati in qualità di Responsabile del trattamento, con particolare attenzione a quei soggetti terzi in outsourcing ed indicare per ognuno di essi il tipo di trattamento effettuato.
Per l'inventario dei soggetti terzi, in outsourcing, deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del trattamento in luogo sicuro.

6.2 - CRITERI PER LA SCELTA DEI SOGGETTI RESPONSABILI DELL'OUTSOURCING
Il Responsabile della sicurezza e del trattamento dei dati può nominare Responsabile del trattamento in outsourcing quei soggetti terzi che abbiano i requisiti individuati all'art. 29 del D.Lgs. n.196/03 (esperienza, capacità, affidabilità).
Il Responsabile del trattamento dei dati in outsourcing deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati, secondo quanto disposto dal D.Lgs. n.196/2003.

6.3 - NOMINA DEL RESPONSABILE DEL TRATTAMENTO IN OUTSOURCING
Per ogni trattamento affidato ad un soggetto esterno nominato Responsabile del trattamento in outsourcing, il Responsabile della sicurezza e del trattamento deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.
Il Responsabile della sicurezza e del trattamento deve informare il responsabile del trattamento dei dati in outsourcing dei compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore ed in particolare di quanto stabilito dal D.Lgs. n.196/2003.
Il Responsabile del trattamento dei dati in outsourcing deve accettare la nomina, utilizzando apposito modulo.
La nomina del Responsabile del trattamento dei dati in outsourcing deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata, a cura del Responsabile della sicurezza e del trattamento dei dati, in luogo sicuro.

## 7. INVENTARI E METODOLOGIE OPERATIVE DI TRATTAMENTO DEI DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare, ad ogni variazione, l'elenco delle tipologie di trattamenti effettuati, in base a quanto comunicatogli dai singoli Responsabili di Settore del trattamento dei dati.
Anche in condizioni di immutata struttura e consistenza o di nessuna variazione delle banche dati soggette al trattamento, la redazione dell'elenco delle basi di dati è soggetto a validazione periodica (come minimo annualmente) e deve essere allegata entro il 31 marzo di ogni anno all'aggiornamento del D.P.P.S
Ogni banca di dati o archivio dovrà essere classificata in relazione alle informazioni in essa contenute indicando se si tratta di:

- Dati personali
- Dati sensibili
- Dati giudiziari

Per l'individuazione degli archivi dei dati oggetto del trattamento dovrà essere utilizzato apposito modulo, che sarà conservato a cura del Responsabile del trattamento dei dati in luogo sicuro.

7.1 - INVENTARIO DELLE SEDI IN CUI SONO TRATTATI I DATI
All'Amministratore di sistema è affidato il compito di aggiornare ad ogni variazione l'elenco delle sedi in cui è effettuato il trattamento dei dati.
Per gestire l'inventario delle sedi in cui sono trattati i dati, dovrà essere utilizzato apposito modulo che dovrà essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro.
Il mantenimento di questo modulo, da produrre in forma cartacea ad ogni aggiornamento annuo del D.P.S., potrà avvenire in maniera informatica e/o mediante uso di software, purché rechi traccia delle indicazioni di inventario delle postazioni hardware deputate al trattamento, degli individui consegnatari e dell'ambiente (locale/ufficio/stanza/area) deputato al trattamento.

7.2 - INVENTARIO DEGLI UFFICI IN CUI SONO TRATTATI I DATI
All'Amministratore di sistema è affidato il compito di aggiornare, ad ogni variazione, l'elenco degli uffici in cui è effettuato il trattamento dei dati.
In particolare, per ogni ufficio dovrà essere indicata la sede e se l'accesso è controllato.
Per l'inventario degli uffici dovrà essere utilizzato apposito modulo che deve essere conservato, a cura del Responsabile del trattamento della sicurezza dei dati, in luogo sicuro.
Il mantenimento di questo modulo, da produrre in forma cartacea ad ogni aggiornamento annuo del D.P.S., potrà avvenire in maniera informatica e/o mediante uso di software purché recante traccia delle indicazioni di inventario delle postazioni hardware deputate al trattamento, degli individui consegnatari e dell'ambiente (locale/ufficio/stanza/area) deputato al trattamento.

7.3 - INVENTARIO DEI SISTEMI DI ELABORAZIONE
All'Amministratore di sistema è affidato il compito di aggiornare, ad ogni variazione, l'elenco dei sistemi di elaborazione con cui è effettuato il trattamento dei dati.
Per ogni sistema saranno descritte le caratteristiche e se si tratta di sistema di elaborazione:

- Non accessibile da altri elaboratori (stand-alone)
- In rete non accessibile al pubblico
- In rete accessibile al pubblico

Ogni altra indicazione di caratteristiche rilevabili dal punto di vista hardware e di rete, quali indirizzi fisici di collegamento, dotazione di specifiche periferiche quali stampanti, scanner, unità dischi esterne, smart-readers di firma digitale ecc. è inoltre consigliata.
Per ogni sistema dovrà essere specificato il nome dell'Incaricato o degli Incaricati che lo utilizzano.
Per l'inventario dei sistemi di elaborazione dovrà essere utilizzato apposito modulo che andrà conservato, a cura del Responsabile del trattamento dei dati, in luogo sicuro.
Il mantenimento di questo modulo, da produrre in forma cartacea ad ogni aggiornamento annuo del D.P.S., può avvenire in maniera informatica e/o mediante uso di software, purché recante traccia delle indicazioni di inventario delle postazioni hardware deputate al trattamento, degli individui consegnatari e dell'ambiente (locale/ufficio/stanza/area) deputato al trattamento.
Questo Comune adotta allo scopo il modulo su Db Access sotto Microsoft Windows® denominato "Rilevazione del censimento Hardware", creato dalla Arionline S.r.l..

## 8. PIANO DI FORMAZIONE DELL'AMMINISTRATORE DI SISTEMA

Al Responsabile della sicurezza e del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione dell'Amministratore di sistema.
Il Responsabile della sicurezza e del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata, fornendone comunicazione adeguata al Titolare del trattamento.

## 9. MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

9.1 - PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI
Ai Responsabili di Settore del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli Incaricati del trattamento autorizzati al trattamento dei dati personali.
In particolare, in caso di trattamento automatizzato di dati, ad ogni Incaricato del trattamento deve essere assegnato uno USER-ID.
Se gestito mediante software automatizzato, lo user-id dovrà cessare automaticamente al 180° giorno di inutilizzo.
In caso di dimissioni di un Incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Responsabile di Settore del trattamento dei dati deve darne immediata comunicazione al Responsabile della sicurezza e del trattamento dei dati, al Custode delle password e all'Amministratore di sistema, i quali a disattiveranno la possibilità di accesso al sistema per il soggetto in questione.
L'elenco degli Incaricati del trattamento deve essere conservato, a cura del Responsabile di Settore del Trattamento dei dati, in luogo sicuro e deve essere trasmesso in copia controllata a:

- Responsabile della Sicurezza e del trattamento dei dati
- Amministratore di sistema
- Custode delle password

9.2 - VERIFICHE PERIODICHE DELLE CONDIZIONI PER LE AUTORIZZAZIONI
All'Amministratore di sistema è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando apposito modulo che deve essere conservato, a cura del Responsabile della sicurezza e del trattamento dei dati, in luogo sicuro.

9.3 - DEFINIZIONE DEI CRITERI DI ASSEGNAZIONE DEI PERMESSI DI ACCESSO AI DATI
Al Responsabile di Settore del trattamento dei dati è affidato il compito di aggiornare ad ogni variazione la tabella dei Permessi di accesso che indica, per ogni banca di dati, i tipi di permesso di accesso per ogni Incaricato del trattamento autorizzato.

In particolare per ogni Incaricato del trattamento e per ogni banca di dati debbono essere indicati i privilegi assegnati tra i seguenti:

- Inserimento di dati
- Lettura e stampa di dati
- Variazione di dati
- Cancellazione di dati

La tabella dei Permessi di accesso deve essere redatta utilizzando l'apposito modulo che deve essere conservato, a cura del Responsabile del trattamento dei dati, in luogo sicuro e deve essere trasmesso in copia controllata a:

- Responsabile della sicurezza e del trattamento dei dati
- Amministratore di sistema

### 9.4 - VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DEI PERMESSI DI ACCESSO AI DATI

Al Responsabile di Settore del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati, utilizzando apposito modulo che deve essere conservato in luogo sicuro e deve essere trasmesso in copia controllata a:

- Responsabile della sicurezza e del trattamento dei dati
- Amministratore di sistema

### 9.5 - PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO

Al Responsabile della sicurezza e del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le necessità di formazione del personale Incaricato del trattamento dei dati, con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati.
Per ogni utente il Responsabile della sicurezza e del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze ed in funzione anche di eventuali variazioni della normativa, le necessità di formazione: queste informazioni devono essere trasmesse in copia controllata al Titolare del trattamento.

## 10. MANUTENZIONE APPARECCHIATURE E SISTEMI DI TRATTAMENTO DEI DATI

### 10.1 - MANUTENZIONE DEI SISTEMI HARDWARE DI ELABORAZIONE DEI DATI

All'Amministratore di sistema è affidato il compito di verificare ogni anno la situazione delle apparecchiature hardware installate con cui sono trattati i dati, delle apparecchiature periferiche ed in particolare dei dispositivi di collegamento con le reti pubbliche (Internet/Intranet).

La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito

Queste verifiche andranno regolarmente effettuate tenendo conto anche dell'evoluzione tecnologica e dell'esistenza di apposite garanzie o contratti di manutenzione con le aziende fornitrici dell'hardware.
L'Amministratore di sistema deve premunirsi, entro il 31 marzo di ogni anno, di relazionare riguardo l'evidenziazione dei rischi legati all'obsolescenza o inaffidabilità dell'hardware.
Nel caso in cui esistano rischi evidenti che possano provocare perdita o impossibilità al regolare svolgimento delle operazioni previste nel D.P.P.S, il Responsabile della sicurezza e del trattamento dei dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

### 10.2 - MANUTENZIONE DEI SISTEMI OPERATIVI

All'Amministratore di sistema, è affidato il compito di verificare, almeno ogni sei mesi, la situazione dei Sistemi Operativi installati sulle apparecchiature con le quali sono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita

- Il rischio di accesso non autorizzato o non consentito

tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

L'Amministratore di sistema deve compilare apposita relazione per l'evidenziazione dei rischi sui Sistemi Operativi.
Nel caso in cui esistano rischi evidenti che possano provocare perdita o impossibilità al regolare svolgimento delle operazioni previste nel D.P.P.S, il Responsabile della sicurezza e del trattamento dei dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

### 10.3 - MANUTENZIONE DELLE APPLICAZIONI SOFTWARE

All'Amministratore di sistema è affidato il compito di verificare, almeno ogni sei mesi, la situazione delle applicazioni installate sulle apparecchiature con cui sono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità del software applicativo, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito
- La regolare esistenza di licenze d'uso e contratti di manutenzione (dove previsti)

Allo scopo dovrà tener conto, in particolare, della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.
L'Amministratore di sistema dovrà compilare una relazione di "Evidenziazione dei rischi nelle applicazioni software" almeno annualmente.
Nel caso in cui esistano rischi evidenti il Responsabile della sicurezza e del trattamento dei dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti per di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

## 11. MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI NON AUTOMATIZZATI O MANUALMENTE SU CARTACEO

Per ogni archivio i Responsabili di Settore del trattamento dei dati debbono definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso degli archivi.

### 11.1 - NOMINA E ISTRUZIONI AGLI INCARICATI

Gli incaricati che trattano atti e documenti che contengono dati personali, sono tenuti a conservarli e restituirli al termine delle operazioni.
Se i documenti contengono dati sensibili e giudiziari (art 4, D.Lgs. n.196/03) gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.
L'accesso agli archivi che contengono documenti dove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, in seguito ad identificazione e registrazione dei soggetti.

### 11.2 - COPIE DEGLI ATTI DEI DOCUMENTI

Quanto indicato nel punto precedente si applica anche a qualunque tipo di copia effettuata sui documenti contenenti dati personali, comprese quelle effettuabili da originali di tipo cartaceo con uso di fotocopiatrici, scanner, macchine digitali, fax o altre unità di riproduzione fotografica, ottica e/o digitale.

## 12. REVISIONI

Questo D.P.S., redatto nel mese di Gennaio del 2006, sarà revisionato annualmente ed eventualmente sottoposto a modifiche, sotto la diretta responsabilità del Responsabile della sicurezza e del trattamento dei dati, entro il 31 marzo di ogni anno.

## DICHIARAZIONE

Tutti gli intervenuti dichiarano di aver preso integrale visione dei compiti previsti per il loro ruolo e accettano le norme di regolamento comportamentale e gli obblighi previsti all'interno di questo D.P.S..

Data: _____

Firme

IL TITOLARE DEL TRATTAMENTO DEI DATI

| | |
|---|---|
| | |

IL RESPONSABILE DELLA SICUREZZA E DEL TRATTAMENTO DEI DATI

| | |
|---|---|
| | |

I RESPONSABILI DI SETTORE DEL TRATTAMENTO DEI DATI:

IL CUSTODE DELLE PASSWORD

| | |
|---|---|
| | |

L'AMMINISTRATORE DI SISTEMA

| | |
|---|---|
| | |

GLI INCARICATI DEL TRATTAMENTO DEI DATI:

| | |
|---|---|
| Anna Maria Pischedda | |
| Zuncheddu Zelinda | |
| Cannas Ignazia | |
| Pusceddu Franco | |
| Zuncheddu Rita | |
| Tolu Angela Maria | |
| Zuncheddu Rita | |
| Vacca Antonello | |
| Corda Antonio | |
| Serra Dino | |
| Serreli Innocenzo | |
| Monni Rosetta | |
| Marcia Maria Carmela | |
| Salvatore Staffa | |