

DOCUMENTO PROGRAMMATICO
PER LA SICUREZZA
AGGIORNAMENTO 2011

COMUNE DI DUNO

INDICE

PREMESSA.....	3
RIFERIMENTI NORMATIVI	3
1. LE FIGURE RILEVANTI:	4
1.a. TITOLARE DEL TRATTAMENTO	4
1.b. RESPONSABILE DEL TRATTAMENTO.....	4
1.c. INCARICATI AL TRATTAMENTO	4
1.d. L'INTERESSATO	4
1.e CUSTODE DELLE PASSWORD.....	5
1.g INCARICATO DELLA MANUTENZIONE DEL SISTEMA	6
2. ORGANIZZAZIONE DEL COMUNE	6
3. RESPONSABILI DEL TRATTAMENTO DEI DATI NEL COMUNE	7
4. ANALISI DEI RISCHI DEL COMUNE	8
4.a DESCRIZIONE DEL SISTEMA INFORMATICO COMUNALE: ANALISI, RISCHI, TABELLE SITUAZIONE	12
MISURE DI SICUREZZA	20
4.b DESCRIZIONE DEL SISTEMA DI ARCHIVIZIONE CARTACEA DEI DATI: ANALISI, RISCHI E MISURE DI SICUREZZA.....	39
5. PROCEDURE DI BACK UP E RIPRISTINO DEI DATI.....	40
6. FORMAZIONE DEL PERSONALE.....	42
7. MODALITA' DI AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA	43

PREMESSA

Il presente documento definisce l'organizzazione e l'attuazione dei principi e delle regole espresse dal Nuovo Codice in materia di protezione dei dati personali, d.lgs. 196/03.

Il Codice prescrive precisi obblighi e comportamenti da attuare nel trattare i dati. Questi sono sanzionabili anche penalmente: è perciò necessario procedere all'adeguamento dell'organizzazione comunale al fine di rispettare le prescrizioni del d.lgs. 196/03.

I principi fondamentali che devono essere alla base di ogni trattamento di dati, intendendo con quest'ultima espressione qualsiasi operazione effettuata con i dati stessi, dalla raccolta, alla conservazione, all'utilizzo fino alla distruzione, sono i seguenti:

- necessità del trattamento;
- liceità del trattamento ed effettuazione dello stesso secondo correttezza;
- esattezza dei dati ed aggiornamento, se necessario, degli stessi;
- completezza, pertinenza e non eccedenza rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
- conservazione in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

La compilazione di un Documento Programmatico sulla Sicurezza da redigere annualmente non è una previsione del tutto nuova rispetto alla normativa precedente. La novità del nuovo codice della privacy 196/03 è l'estensione dell'obbligo della compilazione a tutti i trattamenti di dati sensibili, siano essi in elaboratori accessibili al pubblico o meno.

Il presente Documento Programmatico è redatto, ai sensi degli articoli 33 e seguenti del nuovo Codice sulla privacy e secondo le previsioni del relativo allegato B, per definire e descrivere le politiche di sicurezza adottate dal Comune in materia di trattamento dei dati personali e dei criteri organizzativi seguiti per la loro attuazione e per fornire idonee informazioni a riguardo anche a parti terze.

La tenuta del documento programmatico è una misura minima obbligatoria, la cui violazione comporta sanzioni penali.

RIFERIMENTI NORMATIVI

- A. Decreto Legislativo 29 dicembre 1992 n. 518 (tutela del diritto d'autore sul software)
- B. Codice Penale, in particolare gli articoli introdotti con la legge 547/93 (reati legati all'informatica).
- C. Decreto legislativo 30 giugno 2003 n. 196, Codice per la protezione dei dati personali (c.d. Codice della Privacy - così come modificato dalla Legge 26 febbraio 2004, n. 45, di conversione al D.L. 354/03), ed il suo disciplinare tecnico (allegato B).

1. LE FIGURE RILEVANTI:

1.a. TITOLARE DEL TRATTAMENTO

Il titolare del trattamento è l'Ente Locale, cui competono le decisioni in ordine alla finalità, alle modalità del trattamento, dei dati personali, nonché agli strumenti utilizzati, ivi compreso il profilo della sicurezza (art. 4 comma 1, lett. F) d.lgs.196/03).

1.b. RESPONSABILE DEL TRATTAMENTO

Può essere prevista, in relazione all'attività del titolare del trattamento, la nomina di uno o più responsabili del trattamento, con compiti diversi a seconda delle funzioni svolte.

Il titolare del trattamento può delegare ai responsabili la designazione degli incaricati. Il responsabile del trattamento è individuato tra i soggetti che per esperienza, capacità, affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza (art. 4, comma 1, lett. G) d.lgs. 196/03).

I responsabili del trattamento, inoltre, hanno il compito di controllare, insieme agli amministratori di sistema, ognuno per le proprie specifiche competenze, l'efficacia di programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali e le misure minime di sicurezza; ancora hanno l'obbligo di garantire le misure minime di sicurezza riguardanti i dati del Comune siano rispettate anche nel caso di servizi dati in *outsourcing*.

Per quanto riguarda il comune di DUNO, si veda il capitolo 3 del presente documento.

1.c. INCARICATI AL TRATTAMENTO

Gli incaricati sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. Tali figure operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. Gli incaricati devono essere designati per iscritto previa l'individuazione puntuale dell'ambito del trattamento consentito. (art. 4, comma 1, lett. H) d.lgs. 196/03).

La nomina degli incaricati del trattamento dovrà essere effettuata dai responsabili, utilizzando il modulo allegato al presente documento.

1.d. L'INTERESSATO

È la persona fisica, giuridica, l'ente o l'associazione, cui si riferiscono i dati personali (art. 4, comma 1, lett. I) d.lgs.vo 196/03).

Secondo quanto previsto all'art. 7 del nuovo Codice della privacy, l'interessato ha diritto ad ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati e la loro comunicazione in forma intelligibile.

Inoltre l'interessato ha diritto di ottenere l'indicazione:

- a) dell'origine dei dati;
- b) delle finalità e modalità del trattamento;

MARZO 2011

- c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- d) degli estremi identificativi del titolare, dei responsabili o degli incaricati;
- e) dei soggetti o delle categorie di soggetti ai quali i dati personali devono essere comunicati o che possono venirne a conoscenza.

Ancora, l'interessato ha diritto di ottenere:

- f) l'aggiornamento, la rettificazione o, quando ne ha interesse, l'aggiornamento dei dati;
- g) la cancellazione, la trasformazione in una forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- h) l'attestazione che le operazioni richieste alle lettere f) e g) sono state portate a conoscenza anche per quanto riguarda il loro contenuto a coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso secondo il quale tale adempimento si rivela impossibile o richiede mezzi sproporzionati rispetto al diritto tutelato.

Infine, l'interessato può opporsi a, in tutto o in parte:

- i) per motivi legittimi al trattamento dei dati personali dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- l) al trattamento di dati personali che lo riguardano al fine di invio di materiale pubblicitario o di vendita diretta o per compimento di ricerche di mercato o di comunicazione commerciale.

Per l'esercizio dei diritti di cui sopra, si veda l'art. 8 del D.lgs. 196/03.

1.e CUSTODE DELLE PASSWORD

Si è ritenuto comunque opportuno istituire questa figura, anche se non più obbligatoria ai sensi del Codice della Privacy, per ragioni tecniche e per implementare una migliore politica di sicurezza.

In effetti, con la configurazione software del sistema informatico del Comune, non è possibile introdurre procedure automatizzate e certe che consentano il rispetto delle disposizioni in materia di identificativi e password. Pertanto, si è ritenuto necessario attribuire a una persona fisica le relative mansioni (si veda sotto).

Il custode delle password è individuato nella figura di Sig.ra Alborghetti Giuseppina. Questa figura deve curare tutti gli aspetti relativi alla gestione delle parole chiave, cioè l'assegnazione dei codici identificativi, del cambio periodico delle password ed in particolar modo la custodia di copia delle parole chiave tenute in busta chiusa in luogo segreto.

Tale procedura è illustrata nel dettaglio nella circolare interna n. 4/P, secondo la quale è consentito l'uso del profilo dell'utente solo in necessarie ed improrogabili situazioni di emergenza o di prolungata assenza dell'incaricato che utilizza il computer.

TABELLA 1:Elenco dei trattamenti: informazioni di base

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Descrizione degli strumenti utilizzati	Altre strutture che concorrono al trattamento
		S*	G*			
Servizi alla persona e amministrativo - contabili	Segreteria Ragioneria, tributi ufficio protocollo, assistenza sociale, anagrafe	SI	SI	Area dei servizi alla persona ed amministrativo-contabili	Personal computer, telefono, fax, supporti cartacei	No
Servizi al territorio	Ufficio tecnico ufficio polizia locale,	SI	SI	Area dei servizi al territorio e tributari	Personal computer, telefono, fax, supporti cartacei	No

* LEGENDA:

- S: dati sensibili
- G: dati giudiziari

MARZO 2011

1.f INCARICATO DELLA MANUTENZIONE DEL SISTEMA

Il Comune non ha una completa autonomia gestionale dei sistemi informatici e dell'hardware installato.

Deve, pertanto, utilizzare imprese private esterne con le quali viene creato un rapporto fiduciario.

Il responsabile del trattamento, nello svolgimento delle sue funzioni istituzionali, vigila sulla correttezza di tale rapporto e sulle attività svolte dalle imprese esterne.

In ogni caso, è necessario provvedere all'identificazione fisica degli incaricati della manutenzione e a fargli sottoscrivere una lettera di impegno al rispetto della segretezza dei dati trattati.

2. RESPONSABILE DEL TRATTAMENTO DEI DATI

Il Comune ha nominato/ nominerà mediante apposito decreto il responsabile del trattamento dei dati, nella persona di:

Sig.ra **Alborghetti Giuseppina**

Qualifica Istruttore Amministrativo Contabile - posizione economica C5

che potrà avvalersi, previa autorizzazione, delle eventuali competenze tecniche, giuridico amministrative e logistico – organizzative di cui il comune non è in possesso, mediante specifici accordi con consulenti e/o organizzazioni esterne all'ente

2.a ORGANIZZAZIONE DEL COMUNE

TABELLA 3: Strutture preposte ai trattamenti

Struttura	Responsabile	Trattamenti operati dalla struttura	Compiti della struttura
Servizi affari generali, contratti, segreteria generale, amministrativo tributari.	Dr. Cardillo Giuseppe	Dati di segreteria amministrativa, segreteria generale, gestione tributi locali.	Istruttoria del procedimento e adozione del provvedimento finale salvo procedure tecniche di competenza dell'amministratore di sistema.
Servizi di Ragioneria e Personale.	Dr. Cardillo Giuseppe	Contabilità finanziaria, gestione personale, economo, gestione patrimonio.	Istruttoria del procedimento e adozione del provvedimento finale salvo procedure tecniche di competenza dell'amministratore di sistema
Ufficio servizi demografici e Protocollo	Dr. Cardillo Giuseppe	Dati demografici, anagrafici, relativi a servizi sociali, servizi scolastici, sportivi, turistici, culturali, gestione flussi documentali di protocollo.	Istruttoria del procedimento e adozione del provvedimento finale salvo procedure tecniche di competenza dell'amministratore di sistema.
Area ufficio tecnico	Geom. Vincenti Davide	Dati urbanistica pubblica e privata, piano regolatore, ecologia, smaltimento rifiuti, attività in outsourcing, parchi, giardini, illuminazione, strade pubbliche, manutenzione infrastrutture.	Istruttoria del procedimento e adozione del provvedimento finale salvo procedure tecniche di competenza dell'amministratore di sistema.
Ufficio Polizia	Convenzione con il Comune di	Operazioni di vigilanza, attività di Dati relativi al commercio, artigianato,	Istruttoria del procedimento e adozione del

Documento programmatico per la sicurezza – Comune di Duno

	Cuveglia	fiere e mercati, P.G. assistenza ad altri uffici.	provvedimento finale salvo procedure specifiche di competenza esclusiva del Sindaco.
Ufficio Assistente Sociale	Convenzione con il Comunità Montana Valli del Verbano	Stato di salute, economico e giudiziario dei richiedenti i contributi	raccolta, organizzazione, conservazione, consultazione, modificazione, utilizzo, comunicazione, diffusione, cancellazione di dati inerenti i servizi sociali - amministrativi

3. ANALISI DELLA SITUAZIONE COMUNALE E PROBLEMATICHE GENERALI

Analisi della situazione comunale: problematiche generali

a) strumenti e dotazioni informatiche

Gli strumenti e la dotazione è composta da 2 PC tra di loro collegati in rete **peer-to-peer** (o **P2P**) e di cui uno dei due svolge il ruolo di “Server”.

Vi è inoltre un notebook usato dal Tecnico Comunale anch'esso in rete, quando collegato e presente nella struttura

b) Aspetti logistici e trattamento dati in formato non elettronico

- sicurezza locali: è il problema più evidente in quanto in buona parte degli uffici non sono installati efficaci strumenti antintrusione. Attualmente si evita, quando non vi è il presidio, di lasciare aperti armadi o porte di accesso ai locali interni.
- L'ufficio del sindaco rimane pressoché costantemente aperto, ma essendo solitamente presidiato dal personale è facile controllare le eventuali intrusioni
- Gli arredi, in particolar modo armadi e cassetiere, non appaiono tutti congrui sotto l'aspetto della sicurezza. Non è previsto un sistema di gestione delle chiavi
- L'archivio del Comune non è completamente a norma relativamente ai dettami del 196

c) Personale

- L'organizzazione del personale è congrua sotto l'aspetto gestionale ed operativo

Soluzioni proposte:

a) strumenti e dotazioni informatiche

La dotazione informatica del Comune è stata adeguata per l'aspetto del backup con l'introduzione di “Dischi Removibili” che consentono un salvataggio dei dati in formato nativo e che usati alternativamente (cambio settimanale con ricovero in cassaforte) garantiscono la sicurezza e l'immediata riutilizzabilità dei dati salvati, nonché il ripristino periodico come previsto dalla normativa.

b) Personale

Stante la situazione emersa in fase di indagine si ritiene utile organizzare un corso di aggiornamento, per formare il personale sulle modalità di trattamento dei dati alla luce delle disposizioni normative in essere.

4. ANALISI DEI RISCHI

Per poter programmare efficacemente e realmente una politica di sicurezza, il D.lgs. 196/03 prevede che sia redatta un'attenta analisi dei rischi presenti nel luogo di conservazione dei dati per poter realmente adottare delle misure che siano in grado di ridurre, se non anche eliminare il pericolo.

I rischi presenti per i dati sono di due tipi:

- distruzione, perdita, cancellazione e sottrazione di dati informatici.
- sottrazione, distruzione, perdita di dati in supporti cartacei, siano essi archiviati o meno.

In riferimento ai rischi che minacciano la sicurezza dei dati, il Comune, ha adottato ed intende adottare nel futuro, determinate misure di sicurezza al fine di perseguire i seguenti obiettivi della:

- riservatezza: i dati devono essere accessibili solo alle persone autorizzate. Tale principio, quando applicato dovrebbe essere in grado di ridurre il rischio che persone non autorizzate possano accedere alle informazioni.
- integrità: i dati devono essere protetti da modificazioni e danneggiamenti. Tale principio, quando applicato dovrebbe essere in grado di ridurre il rischio che le informazioni siano non volutamente modificate o cancellate o colposamente perse o distrutte.
- disponibilità: i dati devono essere accessibili alle persone autorizzate. Tale principio, quando applicato dovrebbe ridurre il rischio di non poter accedere ai dati anche se autorizzati dall'amministratore del sistema o dal titolare del trattamento.

4.a DESCRIZIONE DEL SISTEMA INFORMATICO COMUNALE: TABELLE DELLA STRUTTURA INFORMATICA

I

Comune di DUNO	Ufficio Anagrafe / Elettorale		
O.S.:WINDOWS XP PRO			
Procedure di BACKUP e RESTORE			
	ATTIVITA'	SI	NO
Esiste una procedura di BACKUP		SI	
La procedura di BACKUP salva promiscuamente dati sensibili e non		SI	
La procedura di BACKUP avviene per mezzo di un unico Computer		SI	
La procedura di BACKUP e' automatica		SI	
La procedura di BACKUP si avvale di supporti removibili		SI	
Il BACKUP viene controllato periodicamente nell'esito		SI	
I supporti di BACKUP vengono controllati e provati con cadenza periodica		SI	
I supporti di BACKUP vengono sostituiti con cadenza periodica		SI	
I supporti di BACKUP vengono resi inutilizzabili alla loro dismissione		SI	
Il BACKUP e' cifrato in modo da non essere utilizzabile all'esterno della struttura			NO
I supporti di BACKUP vengono conservati in luoghi idonei e controllati nell'accesso		SI	
Il luogo di conservazione dei supporti di backup e' ignifugo e provvisto di serratura			NO
Le procedure di RESTORE vengono provate con cadenza periodica		SI	
In caso di grave disastro si puo' garantire il ripristino dei dati in tempi consoni con i diritti degli interessati		SI	
Inventario Hardware e Software			
	ATTIVITA'	SI	NO
Viene fatto un inventario dell'Hardware presente		SI	
Viene fatto un inventario del Software presente		SI	
L'inventario comprende le locazioni dei dispositivi hardware		SI	
L'inventario comprende le locazioni di installazione dei software		SI	
L'inventario viene aggiornato periodicamente		SI	
Le licenze d'uso del software vengono custodite in luoghi idonei		SI	
Le licenze d'uso del software sono inaccessibili alle persone non autorizzate		SI	
I manuali d'uso dei vari software sono a disposizione per la consultazione da parte del personale		SI	
Esistono delle procedure per l'identificazione ed il recupero del materiale		SI	
Esiste un registro di "carico e scarico" materiali con le relative autorizzazioni			NO
Esiste un inventario delle applicazioni Standard (Office, Windows, ecc...)		SI	
I manuali delle applicazioni Standard sono accessibili da parte degli utenti		SI	
Le applicazioni Standard vengono aggiornate periodicamente per garantire i criteri minimi di sicurezza		SI	
Esiste un inventario delle applicazioni Custom (sviluppi ad Hoc, procedure			NO

Documento programmatico per la sicurezza – Comune di Duno

personalizzate, ecc...)		
I manuali delle applicazioni Custom sono accessibili da parte degli utenti		NO
Le applicazioni Custom vengono aggiornate periodicamente per garantire i criteri minimi di sicurezza		NO
Ruoli Macchine & Utenti		
ATTIVITA'	SI	NO
I computer sui quali avvengono dei trattamenti sono condivisi da più persone	SI	
Le persone che utilizzano lo stesso PC hanno profili omogenei nei trattamenti dei dati	SI	
Le persone che attuano trattamenti ai dati possono avere più profili di trattamento		NO
Gli addetti ai trattamenti sono univocamente definiti all'interno della struttura	SI	
Accessi esterni		
ATTIVITA'	SI	NO
Gli accessi ai sistemi avvengono esclusivamente dall'interno della struttura	SI	
Esistono servizi che devono essere acceduti dall'esterno della struttura		NO
Esistono protezioni per l'impedimento delle intrusioni non autorizzate dall'esterno	SI	
Gli accessi dall'esterno avvengono in maniera cifrata		NO
Gli accessi avvenuti e tentati vengono monitorati e registrati		NO
Procedure di accesso ai dati		
ATTIVITA'	SI	NO
Gli operatori conoscono le procedure di accesso e gestione dei dati secondo il proprio profilo	SI	
Le procedure di accesso ai dati sono redatte anche in forma scritta	SI	
Tali procedure di gestione vengono custodite e controllate da accessi non autorizzati	SI	
Le procedure di gestione subiscono aggiornamenti di forma con cadenza periodica	SI	
Le procedure di gestione scritte vengono aggiornate contestualmente		NO
I dati prelevati vengono comunque depositati al termine dell'orario di apertura (trattamento non concluso)		
I dati prelevati per l'utilizzo vengono depositati solo al termine dell'utilizzo (trattamento concluso)		NO

Comune di DUNO Ufficio Anagrafe / Elettorale			
O.S.: WINDOWS XP PRO			
Gestione Credenziali di Autenticazione - Art. 1 - 10 Allegato B			
ATTIVITA'		SI	NO
Esiste Una Procedura di Autenticazione		SI	
La procedura di autenticazione autentica univocamente il singolo utente all'interno della LAN		SI	
La procedura di autenticazione permette l'accesso al computer locale			NO
Password più Lunghe di 8 caratteri		SI	
Password con Criteri di Complessità		SI	
Le credenziali di accesso ai sistemi sono personali		SI	
Le password sono segrete		SI	
La password viene cambiata almeno ogni 6 mesi		SI	
Le credenziali di accesso ai sistemi non utilizzate da almeno sei mesi vengono disabilitate		SI	
Le credenziali di accesso ai sistemi vengono disabilitate se il titolare non ha più diritto all'utilizzo		SI	
gli utenti sono formati all'utilizzo sicuro del terminale (es. non lasciare sessioni aperte incustodite)		SI	
Esiste una procedura per poter utilizzare comunque le credenziali di un dipendente indisponibile		SI	
La custodia delle copie delle credenziali di accesso ai sistemi è organizzata garantendo la segretezza		SI	
Sistemi di Autorizzazione Art. 12 - 14 Allegato B			
ATTIVITA'		SI	NO
Sono individuati profili di autorizzazione di ambito diverso		SI	
I profili di autorizzazione sono stati creati prima dell'inizio del trattamento dei dati		SI	
Viene verificato lo stato delle condizioni per la conservazione dei profili di autorizzazione		SI	
Altre Misure di Sicurezza Art. 15 - 18 Allegato B			
ATTIVITA'		SI	NO
I dati personali sono protetti contro il rischio di intrusione		SI	
I sistemi antiintrusione (firewall, antivirus, vpn) sono controllati e/o aggiornati semestralmente		SI	
I software con cui vengono trattati i dati vengono aggiornati annualmente		SI	
I software con cui vengono trattati i dati sensibili vengono aggiornati semestralmente		SI	
Sono presenti sistemi di salvataggio dei dati (Nastri, CD, DVD)		SI	

Documento programmatico per la sicurezza – Comune di Duno

Il personale e' addestrato al salvataggio dei dati (backup)	SI	
Il personale esegue il salvataggio dei dati (backup) almeno settimanalmente	SI	
Ulteriori Misure in caso di trattamento di dati sensibili e giudiziari Art. 20 - 24 Allegato B		
ATTIVITA'	SI	NO
Vengono trattabili dati sensibili o giudiziari	SI	
I dati sensibili o giudiziari sono protetti contro l'accesso abusivo	SI	
Vengono utilizzati supporti rimuovibili nel trattamento dei dati sensibili o giudiziari		NO
Il personale è addestrato alla custodia e al mantenimento dei supporti rimuovibili sui quali sono mantenuti i dati		--
I supporti rimuovibili contenenti dati sensibili o giudiziari vengono resi inutilizzabili alla loro dismissione		--
I sistemi di ripristino dei dati svolgono efficientemente il loro compito		--
In caso di bisogno i dati sensibili o giudiziari sono accessibili con tempi compatibili con i diritti degli interessati		--
Misure di tutela e garanzie Art. 25 - 26 Allegato B		
ATTIVITA'	SI	NO
Esistono la documentazione e un disciplinare tecnico per ogni intervento effettuato da terzi in materia di sicurezza		NO
Trattamento senza strumenti informatici Art. 27 - 29 Allegato B		
ATTIVITA'	SI	NO
Si trattano dati sensibili in formato non elettronico	SI	
Gli incaricati sono istruiti per il controllo e la custodia dei dati sensibili	SI	
Gli incaricati adibiti ad un particolare ambito vengono cambiati con una data frequenza		NO
Gli incaricati, per la durata dei loro compiti, controllano e custodiscono i dati in maniera da evitare accessi non autorizzati	SI	
Gli incaricati al termine dei compiti restituiscono i dati nelle struttura preposte all'archiviazione	SI	
L'accesso agli archivi e' controllato	SI	
Qualora un incaricato acceda agli archivi oltre l'orario di apertura questo viene identificato e registrato		NO
Gli incaricati per l'accesso ai dati sensibili devono essere preventivamente autorizzati	SI	

Comune di DUNO Ufficio Ragioneria/Tributi/Personale		
O.S.: WINDOWS XP PRO		
Procedure di BACKUP e RESTORE		
ATTIVITA'	SI	NO
Esiste una procedura di BACKUP	SI	
La procedura di BACKUP salva promiscuamente dati sensibili e non	SI	
La procedura di BACKUP avviene per mezzo di un unico Computer	SI	
La procedura di BACKUP e' automatica	SI	
La procedura di BACKUP si avvale di supporti removibili	SI	
Il BACKUP viene controllato periodicamente nell'esito	SI	
I supporti di BACKUP vengono controllati e provati con cadenza periodica	SI	
I supporti di BACKUP vengono sostituiti con cadenza periodica	SI	
I supporti di BACKUP vengono resi inutilizzabili alla loro dismissione	SI	
Il BACKUP e' cifrato in modo da non essere utilizzabile all'esterno della struttura		NO
I supporti di BACKUP vengono conservati in luoghi idonei e controllati nell'accesso	SI	
Il luogo di conservazione dei supporti di backup e' ignifugo e provvisto di serratura		NO
Le procedure di RESTORE vengono provate con cadenza periodica	SI	
In caso di grave disastro si può garantire il ripristino dei dati in tempi consoni con i diritti degli interessati	SI	
Inventario Hardware e Software		
ATTIVITA'	SI	NO
Viene fatto un inventario dell'Hardware presente	SI	
Viene fatto un inventario del Software presente	SI	
L'inventario comprende le locazioni dei dispositivi hardware	SI	
L'inventario comprende le locazioni di installazione dei software	SI	
L'inventario viene aggiornato periodicamente	SI	
Le licenze d'uso del software vengono custodite in luoghi idonei	SI	
Le licenze d'uso del software sono inaccessibili alle persone non autorizzate		NO
I manuali d'uso dei vari software sono a disposizione per la consultazione da parte del personale	SI	
Esistono delle procedure per l'identificazione ed il recupero del materiale	SI	
Esiste un registro di "carico e scarico" materiali con le relative autorizzazioni		NO
Esiste un inventario delle applicazioni Standard (Office, Windows, ecc...)	SI	
I manuali delle applicazioni Standard sono accessibili da parte degli utenti	SI	
Le applicazioni Standard vengono aggiornate periodicamente per garantire i criteri minimi di sicurezza	SI	
Esiste un inventario delle applicazioni Custom (sviluppi ad Hoc, procedure personalizzate, ecc...)		NO
I manuali delle applicazioni Custom sono accessibili da parte degli utenti		NO

Documento programmatico per la sicurezza – Comune di Duno

Le applicazioni Custom vengono aggiornate periodicamente per garantire i criteri minimi di sicurezza			NO
Ruoli Macchine & Utenti			
ATTIVITA'			
I computer sui quali avvengono dei trattamenti sono condivisi da più persone	SI		NO
Le persone che utilizzano lo stesso PC hanno profili omogenei nei trattamenti dei dati	SI		
Le persone che attuano trattamenti ai dati possono avere più profili di trattamento			NO
Gli addetti ai trattamenti sono univocamente definiti all'interno della struttura	SI		
Accessi esterni			
ATTIVITA'			
Gli accessi ai sistemi avvengono esclusivamente dall'interno della struttura	SI		
Esistono servizi che devono essere acceduti dall'esterno della struttura			NO
Esistono protezioni per l'impedimento delle intrusioni non autorizzate dall'esterno	SI		
Gli accessi dall'esterno avvengono in maniera cifrata			NO
Gli accessi avvenuti e tentati vengono monitorati e registrati			NO
Procedure di accesso ai dati			
ATTIVITA'			
Gli operatori conoscono le procedure di accesso e gestione dei dati secondo il proprio profilo	SI		
Le procedure di accesso ai dati sono redatte anche in forma scritta	SI		
Tali procedure di gestione vengono custodite e controllate da accessi non autorizzati	SI		
Le procedure di gestione subiscono aggiornamenti di forma con cadenza periodica	SI		
Le procedure di gestione scritte vengono aggiornate contestualmente			NO
I dati prelevati vengono comunque depositati al termine dell'orario di apertura (trattamento non concluso)			
I dati prelevati per l'utilizzo vengono depositati solo al termine dell'utilizzo (trattamento concluso)			NO

Documento programmatico per la sicurezza – Comune di Duno

Comune di DUNO	Ufficio Ragioneria/Tributi/Personale		
O.S.: WINDOWS XP PRO			
Gestione Credenziali di Autenticazione Art. 1 - 10 Allegato B			
ATTIVITA'		SI	NO
Esiste Una Procedura di Autenticazione		SI	
La procedura di autenticazione autentica univocamente il singolo utente all'interno della LAN		SI	
La procedura di autenticazione permette l'accesso al computer locale			NO
Password più Lunghe di 8 caratteri		SI	
Password con Criteri di Complessità		SI	
Le credenziali di accesso ai sistemi sono personali		SI	
Le password sono segrete		SI	
La password viene cambiata almeno ogni 6 mesi		SI	
Le credenziali di accesso ai sistemi non utilizzate da almeno sei mesi vengono disabilitate		SI	
Le credenziali di accesso ai sistemi vengono disabilitate se il titolare non ha più diritto all'utilizzo		SI	
gli utenti sono formati all'utilizzo sicuro del terminale (es. non lasciare sessioni aperte incustodite)		SI	
Esiste una procedura per poter utilizzare comunque le credenziali di un dipendente indisponibile		SI	
La custodia delle copie delle credenziali di accesso ai sistemi è organizzata garantendo la segretezza		SI	
Sistemi di Autorizzazione Art. 12 - 14 Allegato B			
ATTIVITA'		SI	NO
Sono individuati profili di autorizzazione di ambito diverso		SI	
I profili di autorizzazione sono stati creati prima dell'inizio del trattamento dei dati		SI	
Viene verificato lo stato delle condizioni per la conservazione dei profili di autorizzazione		SI	
Altre Misure di Sicurezza Art. 15 - 18 Allegato B			
ATTIVITA'		SI	NO
I dati personali sono protetti contro il rischio di intrusione		SI	
I sistemi antiintrusione (firewall, antivirus, vpn) sono controllati e/o aggiornati semestralmente		SI	
I software con cui vengono trattati i dati vengono aggiornati annualmente		SI	
I software con cui vengono trattati i dati sensibili vengono aggiornati semestralmente		SI	
Sono presenti sistemi di salvataggio dei dati (Nastri, CD, DVD)		SI	
Il personale e' addestrato al salvataggio dei dati (backup)		SI	
Il personale esegue il salvataggio dei dati (backup) almeno settimanalmente		SI	

Documento programmatico per la sicurezza – Comune di Duno

Ulteriori Misure in caso di trattamento di dati sensibili e giudiziari Art. 20 - 24 Allegato B		
ATTIVITA'	SI	NO
Vengono trattabili dati sensibili o giudiziari	SI	
I dati sensibili o giudiziari sono protetti contro l'accesso abusivo	SI	
Vengono utilizzati supporti rimuovibili nel trattamento dei dati sensibili o giudiziari		NO
Il personale è addestrato alla custodia e al mantenimento dei supporti rimuovibili sui quali sono mantenuti i dati		--
I supporti rimuovibili contenenti dati sensibili o giudiziari vengono resi inutilizzabili alla loro dismissione		--
I sistemi di ripristino dei dati svolgono efficientemente il loro compito		--
In caso di bisogno i dati sensibili o giudiziari sono accessibili con tempi compatibili con i diritti degli interessati		--
Misure di tutela e garanzie Art. 25 - 26 Allegato B		
ATTIVITA'	SI	NO
Esistono la documentazione e un disciplinare tecnico per ogni intervento effettuato da terzi in materia di sicurezza		NO
Trattamento senza strumenti informatici Art. 27 - 29 Allegato B		
ATTIVITA'	SI	NO
Si trattano dati sensibili in formato non elettronico	SI	
Gli incaricati sono istruiti per il controllo e la custodia dei dati sensibili	SI	
Gli incaricati adibiti ad un particolare ambito vengono cambiati con una data frequenza		NO
Gli incaricati, per la durata dei loro compiti, controllano e custodiscono i dati in maniera da evitare accessi non autorizzati	SI	
Gli incaricati al termine dei compiti restituiscono i dati nelle struttura preposte all'archiviazione	SI	
L'accesso agli archivi e' controllato	SI	
Qualora un incaricato acceda agli archivi oltre l'orario di apertura questo viene identificato e registrato		NO
Gli incaricati per l'accesso ai dati sensibili devono essere preventivamente autorizzati	SI	

Comune di DUNO Ufficio Affari Generali /Segretario Comunale/Protocollo		
O.S.: WINDOWS XP PRO		
Procedure di BACKUP e RESTORE		
ATTIVITA'	SI	NO
Esiste una procedura di BACKUP	SI	
La procedura di BACKUP salva promiscuamente dati sensibili e non	SI	
La procedura di BACKUP avviene per mezzo di un unico Computer	SI	
La procedura di BACKUP e' automatica	SI	
La procedura di BACKUP si avvale di supporti removibili	SI	
Il BACKUP viene controllato periodicamente nell'esito	SI	
I supporti di BACKUP vengono controllati e provati con cadenza periodica	SI	
I supporti di BACKUP vengono sostituiti con cadenza periodica	SI	
I supporti di BACKUP vengono resi inutilizzabili alla loro dismissione	SI	
Il BACKUP e' cifrato in modo da non essere utilizzabile all'esterno della struttura		NO
I supporti di BACKUP vengono conservati in luoghi idonei e controllati nell'accesso	SI	
Il luogo di conservazione dei supporti di backup e' ignifugo e provvisto di serratura		NO
Le procedure di RESTORE vengono provate con cadenza periodica	SI	
In caso di grave disastro si puo' garantire il ripristino dei dati in tempi consoni con i diritti degli interessati	SI	
Inventario Hardware e Software		
ATTIVITA'	SI	NO
Viene fatto un inventario dell'Hardware presente	SI	
Viene fatto un inventario del Software presente	SI	
L'inventario comprende le locazioni dei dispositivi hardware	SI	
L'inventario comprende le locazioni di installazione dei software	SI	
L'inventario viene aggiornato periodicamente	SI	
Le licenze d'uso del software vengono custodite in luoghi idonei	SI	
Le licenze d'uso del software sono inaccessibili alle persone non autorizzate		NO
I manuali d'uso dei vari software sono a disposizione per la consultazione da parte del personale	SI	
Esistono delle procedure per l'identificazione ed il recupero del materiale	SI	
Esiste un registro di "carico e scarico" materiali con le relative autorizzazioni		NO
Esiste un inventario delle applicazioni Standard (Office, Windows, ecc...)	SI	
I manuali delle applicazioni Standard sono accessibili da parte degli utenti	SI	
Le applicazioni Standard vengono aggiornate periodicamente per garantire i criteri minimi di sicurezza	SI	
Esiste un inventario delle applicazioni Custom (sviluppi ad Hoc, procedure personalizzate, ecc...)		NO
I manuali delle applicazioni Custom sono accessibili da parte degli utenti		NO

Documento programmatico per la sicurezza – Comune di Duno

Le applicazioni Custom vengono aggiornate periodicamente per garantire i criteri minimi di sicurezza			NO
Ruoli Macchine & Utenti			
ATTIVITA'			
I computer sui quali avvengono dei trattamenti sono condivisi da più persone	SI		NO
Le persone che utilizzano lo stesso PC hanno profili omogenei nei trattamenti dei dati	SI		
Le persone che attuano trattamenti ai dati possono avere più profili di trattamento			NO
Gli addetti ai trattamenti sono univocamente definiti all'interno della struttura	SI		
Accessi esterni			
ATTIVITA'			
Gli accessi ai sistemi avvengono esclusivamente dall'interno della struttura	SI		
Esistono servizi che devono essere acceduti dall'esterno della struttura			NO
Esistono protezioni per l'impedimento delle intrusioni non autorizzate dall'esterno	SI		
Gli accessi dall'esterno avvengono in maniera cifrata			NO
Gli accessi avvenuti e tentati vengono monitorati e registrati			NO
Procedure di accesso ai dati			
ATTIVITA'			
Gli operatori conoscono le procedure di accesso e gestione dei dati secondo il proprio profilo	SI		
Le procedure di accesso ai dati sono redatte anche in forma scritta	SI		
Tali procedure di gestione vengono custodite e controllate da accessi non autorizzati	SI		
Le procedure di gestione subiscono aggiornamenti di forma con cadenza periodica	SI		
Le procedure di gestione scritte vengono aggiornate contestualmente			NO
I dati prelevati vengono comunque depositati al termine dell'orario di apertura (trattamento non concluso)			
I dati prelevati per l'utilizzo vengono depositati solo al termine dell'utilizzo (trattamento concluso)			NO

Comune di DUNO Ufficio Affari Generali /Segretario Comunale/Protocollo		
O.S.: WINDOWS XP PRO		
Gestione Credenziali di Autenticazione Art. 1 - 10 Allegato B		
ATTIVITA'	SI	NO
Esiste Una Procedura di Autenticazione	SI	
La procedura di autenticazione autentica univocamente il singolo utente all'interno della LAN	SI	
La procedura di autenticazione permette l'accesso al computer locale		NO
Password più Lunghe di 8 caratteri	SI	
Password con Criteri di Complessità	SI	
Le credenziali di accesso ai sistemi sono personali	SI	
Le password sono segrete	SI	
La password viene cambiata almeno ogni 6 mesi	SI	
Le credenziali di accesso ai sistemi non utilizzate da almeno sei mesi vengono disabilitate	SI	
Le credenziali di accesso ai sistemi vengono disabilitate se il titolare non ha più diritto all'utilizzo	SI	
gli utenti sono formati all'utilizzo sicuro del terminale (es. non lasciare sessioni aperte incustodite)	SI	
Esiste una procedura per poter utilizzare comunque le credenziali di un dipendente indisponibile	SI	
La custodia delle copie delle credenziali di accesso ai sistemi è organizzata garantendo la segretezza	SI	
Sistemi di Autorizzazione Art. 12 - 14 Allegato B		
ATTIVITA'	SI	NO
Sono individuati profili di autorizzazione di ambito diverso	SI	
I profili di autorizzazione sono stati creati prima dell'inizio del trattamento dei dati	SI	
Viene verificato lo stato delle condizioni per la conservazione dei profili di autorizzazione	SI	
Altre Misure di Sicurezza Art. 15 - 18 Allegato B		
ATTIVITA'	SI	NO
I dati personali sono protetti contro il rischio di intrusione	SI	
I sistemi antiintrusione (firewall, antivirus, vpn) sono controllati e/o aggiornati semestralmente	SI	
I software con cui vengono trattati i dati vengono aggiornati annualmente	SI	
I software con cui vengono trattati i dati sensibili vengono aggiornati semestralmente	SI	
Sono presenti sistemi di salvataggio dei dati (Nastri, CD, DVD)	SI	
Il personale e' addestrato al salvataggio dei dati (backup)	SI	

Documento programmatico per la sicurezza – Comune di Duno

Il personale esegue il salvataggio dei dati (backup) almeno settimanalmente	SI	
Ulteriori Misure in caso di trattamento di dati sensibili e giudiziari Art. 20 - 24 Allegato B		
ATTIVITA'	SI	NO
Vengono trattabili dati sensibili o giudiziari	SI	
I dati sensibili o giudiziari sono protetti contro l'accesso abusivo	SI	
Vengono utilizzati supporti rimuovibili nel trattamento dei dati sensibili o giudiziari		NO
Il personale è addestrato alla custodia e al mantenimento dei supporti rimuovibili sui quali sono mantenuti i dati		--
I supporti rimuovibili contenenti dati sensibili o giudiziari vengono resi inutilizzabili alla loro dismissione		--
I sistemi di ripristino dei dati svolgono efficientemente il loro compito		--
In caso di bisogno i dati sensibili o giudiziari sono accessibili con tempi compatibili con i diritti degli interessati		--
Misure di tutela e garanzie Art. 25 - 26 Allegato B		
ATTIVITA'	SI	NO
Esistono la documentazione e un disciplinare tecnico per ogni intervento effettuato da terzi in materia di sicurezza		NO
Trattamento senza strumenti informatici Art. 27 - 29 Allegato B		
ATTIVITA'	SI	NO
Si trattano dati sensibili in formato non elettronico	SI	
Gli incaricati sono istruiti per il controllo e la custodia dei dati sensibili	SI	
Gli incaricati adibiti ad un particolare ambito vengono cambiati con una data frequenza		NO
Gli incaricati, per la durata dei loro compiti, controllano e custodiscono i dati in maniera da evitare accessi non autorizzati	SI	
Gli incaricati al termine dei compiti restituiscono i dati nelle struttura preposte all'archiviazione	SI	
L'accesso agli archivi e' controllato	SI	
Qualora un incaricato acceda agli archivi oltre l'orario di apertura questo viene identificato e registrato		NO
Gli incaricati per l'accesso ai dati sensibili devono essere preventivamente autorizzati	SI	

Documento programmatico per la sicurezza – Comune di Duno

Comune di DUNO	Ufficio Tecnico		
O.S.: WINDOWS XP PRO			
Procedure di BACKUP e RESTORE			
ATTIVITA'		SI	NO
Esiste una procedura di BACKUP		SI	
La procedura di BACKUP salva promiscuamente dati sensibili e non		SI	
La procedura di BACKUP avviene per mezzo di un unico Computer		SI	
La procedura di BACKUP e' automatica		SI	
La procedura di BACKUP si avvale di supporti removibili		SI	
Il BACKUP viene controllato periodicamente nell'esito		SI	
I supporti di BACKUP vengono controllati e provati con cadenza periodica		SI	
I supporti di BACKUP vengono sostituiti con cadenza periodica		SI	
I supporti di BACKUP vengono resi inutilizzabili alla loro dismissione		SI	
Il BACKUP e' cifrato in modo da non essere utilizzabile all'esterno della struttura			NO
I supporti di BACKUP vengono conservati in luoghi idonei e controllati nell'accesso		SI	
Il luogo di conservazione dei supporti di backup e' ignifugo e provvisto di serratura			NO
Le procedure di RESTORE vengono provate con cadenza periodica		SI	
In caso di grave disastro si può garantire il ripristino dei dati in tempi consoni con i diritti degli interessati		SI	
Inventario Hardware e Software			
ATTIVITA'		SI	NO
Viene fatto un inventario dell'Hardware presente		SI	
Viene fatto un inventario del Software presente		SI	
L'inventario comprende le locazioni dei dispositivi hardware		SI	
L'inventario comprende le locazioni di installazione dei software		SI	
L'inventario viene aggiornato periodicamente		SI	
Le licenze d'uso del software vengono custodite in luoghi idonei		SI	
Le licenze d'uso del software sono inaccessibili alle persone non autorizzate			NO
I manuali d'uso dei vari software sono a disposizione per la consultazione da parte del personale		SI	
Esistono delle procedure per l'identificazione ed il recupero del materiale		SI	
Esiste un registro di "carico e scarico" materiali con le relative autorizzazioni			NO
Esiste un inventario delle applicazioni Standard (Office, Windows, ecc...)		SI	
I manuali delle applicazioni Standard sono accessibili da parte degli utenti		SI	
Le applicazioni Standard vengono aggiornate periodicamente per garantire i criteri minimi di sicurezza		SI	
Esiste un inventario delle applicazioni Custom (sviluppi ad Hoc, procedure personalizzate, ecc...)			NO
I manuali delle applicazioni Custom sono accessibili da parte degli utenti			NO
Le applicazioni Custom vengono aggiornate periodicamente per garantire i criteri minimi di sicurezza			NO

Documento programmatico per la sicurezza – Comune di Duno

Ruoli Macchine & Utenti		
ATTIVITA'	SI	NO
I computer sui quali avvengono dei trattamenti sono condivisi da più persone	SI	
Le persone che utilizzano lo stesso PC hanno profili omogenei nei trattamenti dei dati	SI	
Le persone che attuano trattamenti ai dati possono avere più profili di trattamento		NO
Gli addetti ai trattamenti sono univocamente definiti all'interno della struttura	SI	
Accessi esterni		
ATTIVITA'	SI	NO
Gli accessi ai sistemi avvengono esclusivamente dall'interno della struttura	SI	
Esistono servizi che devono essere acceduti dall'esterno della struttura		NO
Esistono protezioni per l'impedimento delle intrusioni non autorizzate dall'esterno	SI	
Gli accessi dall'esterno avvengono in maniera cifrata		NO
Gli accessi avvenuti e tentati vengono monitorati e registrati		NO
Procedure di accesso ai dati		
ATTIVITA'	SI	NO
Gli operatori conoscono le procedure di accesso e gestione dei dati secondo il proprio profilo	SI	
Le procedure di accesso ai dati sono redatte anche in forma scritta	SI	
Tali procedure di gestione vengono custodite e controllate da accessi non autorizzati	SI	
Le procedure di gestione subiscono aggiornamenti di forma con cadenza periodica	SI	
Le procedure di gestione scritte vengono aggiornate contestualmente		NO
I dati prelevati vengono comunque depositati al termine dell'orario di apertura (trattamento non concluso)		
I dati prelevati per l'utilizzo vengono depositati solo al termine dell'utilizzo (trattamento concluso)		NO

Comune di DUNO Ufficio Tecnico			
O.S.: WINDOWS XP PRO			
Gestione Credenziali di Autenticazione Art. 1 - 10 Allegato B			
ATTIVITA'		SI	NO
Esiste Una Procedura di Autenticazione		SI	
La procedura di autenticazione autentica univocamente il singolo utente all'interno della LAN		SI	
La procedura di autenticazione permette l'accesso al computer locale			NO
Password più Lunghe di 8 caratteri		SI	
Password con Criteri di Complessità		SI	
Le credenziali di accesso ai sistemi sono personali		SI	
Le password sono segrete		SI	
La password viene cambiata almeno ogni 6 mesi		SI	
Le credenziali di accesso ai sistemi non utilizzate da almeno sei mesi vengono disabilitate		SI	
Le credenziali di accesso ai sistemi vengono disabilitate se il titolare non ha più diritto all'utilizzo		SI	
gli utenti sono formati all'utilizzo sicuro del terminale (es. non lasciare sessioni aperte incustodite)		SI	
Esiste una procedura per poter utilizzare comunque le credenziali di un dipendente indisponibile		SI	
La custodia delle copie delle credenziali di accesso ai sistemi è organizzata garantendo la segretezza		SI	
Sistemi di Autorizzazione Art. 12 - 14 Allegato B			
ATTIVITA'		SI	NO
Sono individuati profili di autorizzazione di ambito diverso		SI	
I profili di autorizzazione sono stati creati prima dell'inizio del trattamento dei dati		SI	
Viene verificato lo stato delle condizioni per la conservazione dei profili di autorizzazione		SI	
Altre Misure di Sicurezza Art. 15 - 18 Allegato B			
ATTIVITA'		SI	NO
I dati personali sono protetti contro il rischio di intrusione		SI	
I sistemi antiintrusione (firewall, antivirus, vpn) sono controllati e/o aggiornati semestralmente		SI	
I software con cui vengono trattati i dati vengono aggiornati annualmente		SI	
I software con cui vengono trattati i dati sensibili vengono aggiornati semestralmente		SI	
Sono presenti sistemi di salvataggio dei dati (Nastri, CD, DVD)		SI	
Il personale e' addestrato al salvataggio dei dati (backup)		SI	

Documento programmatico per la sicurezza – Comune di Duno

Il personale esegue il salvataggio dei dati (backup) almeno settimanalmente	SI	
Ulteriori Misure in caso di trattamento di dati sensibili e giudiziari Art. 20 - 24 Allegato B		
ATTIVITA'	SI	NO
Vengono trattabili dati sensibili o giudiziari	SI	
I dati sensibili o giudiziari sono protetti contro l'accesso abusivo	SI	
Vengono utilizzati supporti rimuovibili nel trattamento dei dati sensibili o giudiziari		NO
Il personale è addestrato alla custodia e al mantenimento dei supporti rimuovibili sui quali sono mantenuti i dati		--
I supporti rimuovibili contenenti dati sensibili o giudiziari vengono resi inutilizzabili alla loro dismissione		--
I sistemi di ripristino dei dati svolgono efficientemente il loro compito		--
In caso di bisogno i dati sensibili o giudiziari sono accessibili con tempi compatibili con i diritti degli interessati		--
Misure di tutela e garanzie Art. 25 - 26 Allegato B		
ATTIVITA'	SI	NO
Esistono la documentazione e un disciplinare tecnico per ogni intervento effettuato da terzi in materia di sicurezza	SI	
Trattamento senza strumenti informatici Art. 27 - 29 Allegato B		
ATTIVITA'	SI	NO
Si trattano dati sensibili in formato non elettronico	SI	
Gli incaricati sono istruiti per il controllo e la custodia dei dati sensibili	SI	
Gli incaricati adibiti ad un particolare ambito vengono cambiati con una data frequenza		NO
Gli incaricati, per la durata dei loro compiti, controllano e custodiscono i dati in maniera da evitare accessi non autorizzati	SI	
Gli incaricati al termine dei compiti restituiscono i dati nelle struttura preposte all'archiviazione	SI	
L'accesso agli archivi e' controllato	SI	
Qualora un incaricato acceda agli archivi oltre l'orario di apertura questo viene identificato e registrato		NO
Gli incaricati per l'accesso ai dati sensibili devono essere preventivamente autorizzati	SI	

TABELLA di Analisi dei rischi

Evento		Impatto sulla sicurezza dei dati		Riferimento alle misure di sicurezza
		Descrizione delle conseguenze dell'evento	Gravità stimata ¹	
Comportamenti degli operatori	Furto di credenziali di autenticazione	Accesso illegittimo al sistema informatico, manipolazione, cancellazione, sottrazione dei dati, comunicazione o diffusione degli stessi.	5	7)
	Carenza di consapevolezza, disattenzione o incuria	Errata custodia dei dati, trattamento illecito, aumento della possibilità di furto, cancellazione, sottrazione o distruzione dei dati e altre conseguenze che determinino una condizione di pericolo per i dati.	5	4), 6), 7), 9)

¹ La gravità è stimata in una scala di valori da 1 a 10.

	Comportamenti sleali o fraudolenti	Sottrazione, cancellazione, manipolazione dei dati, comunicazione o diffusione a terzi.	9	2)
	Errore materiale	Perdita, cancellazione o modifica dei dati.	7	4), 7)
Eventi relativi agli strumenti	Azione di virus informatici o di trojan horse	Accessi abusivi, cancellazione o manipolazione dei dati, blocco dei sistemi hardware e software.	7	3)
	Spamming o altre tecniche di sabotaggio	Blocco dei sistemi operativi, cancellazione, sottrazione o manipolazione dei dati.	6	4), 6), 7)
	Malfunzionamento, indisponibilità o degrado degli strumenti	Aumento delle circostanze di pericolo dovute a strumenti non in grado di assicurare una politica di sicurezza efficace.	7	1)
	Accessi esterni non autorizzati	Accesso illegittimo al sistema informatico, manipolazione, cancellazione, Sottrazione dei dati, comunicazione o diffusione degli stessi.	8	3), 9)

	Intercettazioni di informazioni in rete	Diffusione e comunicazione a terzi non autorizzati di dati, sottrazione o manipolazione degli stessi.	2	5)
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto (archivi)	Accesso illegittimo, manipolazione, cancellazione, Sottrazione dei dati, comunicazione o diffusione degli stessi.	9	8), 9)
	Asportazione e furto di strumenti contenenti dati	Accesso abusivo ai dati contenuti nello strumento oggetto di furto con conseguente accesso ai dati, possibile manipolazione, cancellazione di essi.	7	8)
	Eventi distruttivi, naturali o artificiali (terremoto, inondazione, fulmini, incendio...), dolosi, accidentali o dovuti ad incuria.	Distruzione totale o parziale dei dati, irrecuperabilità degli stessi.	10	1)

	Guasto ai sistemi complementari (ad es.: impianto elettrico, la climatizzazione entrerà in funzione nella nuova sede comunale, a luglio 2004)	Perdita totale o parziale dei dati, danneggiamento dei sistemi di trattamento dei dati.	9	1), 7)
	Errori umani nella gestione della sicurezza fisica.	Accesso illegittimo al sistema informatico e non informatico, manipolazione, cancellazione, sottrazione dei dati, comunicazione o diffusione degli stessi.	7	2), 1), 9)

Tabelle di analisi dei flussi documentali

DUNO: FLUSSI DOCUMENTALI	
in che modo comunicano con l'esterno	albo pretorio, bacheca, affissioni
in che modo comunicano fra di loro (voce, scritti, posta interna, mail, ecc.)	verbalmente
che tipo di documentazione ricevono dall'esterno e su che supporto.	documenti per posta o su formato elettronico.
esiste un punto di smistamento comune per la corrispondenza in entrata?	Ufficio protocollo apre anche la posta sensibile- protocollo informatico non regolamentato, manca il manuale di gestione non smistamento manuale e cartaceo.
esiste un punto di smistamento comune per la corrispondenza in uscita?	Ufficio protocollo. Smistamento non sicuro e non regolamentato. Atti riservati portati direttamente al protocollo.
la posta in entrata viene visionata esclusivamente dal soggetto a cui è indirizzata?	No
la comunicazione interna avviene per mezzo di:	
voce	si
documenti scritti	no
sistema di posta interna	no
mail	Si
Caselle	Aperte e accessibili
come avviene il passaggio di documenti da un operatore comunale all'altro?	Sistemi tradizionali. Non viene tracciato il percorso
ogni impiegato ha inoltre un indirizzo di posta per ufficio a cui possono arrivare le mail di richiesta dall'esterno	Caselle email per funzioni ed ufficio
esiste un indirizzo INFO generico di cui si occupa il protocollo	Si e anche di posta certificata

MARZO 2011

Tabella della struttura organizzativa

DUNO		STRUTTURA ORGANIZZATIVA		
UFFICIO	UTENTE	TIPO DI DATI TRATTATI		
		PERSONALI	SENSIBILI	GIUDIZIARI
uff. anagrafe	ALBORGHETTI GIUSEPPINA	si	si	si
uff. ragioneria	ALBORGHETTI GIUSEPPINA	si	si	si
uff. tecnico	Geom.VINCENTI DAVIDE	si	si	si
uff. sindaco	Ing. PAGLIA PIETRO	si	si	si
uff. segretario	Dr. CARDILLO GIUSEPPE	si	si	si

4.a MISURE DI SICUREZZA

Il Comune ha deciso l'adozione delle misure minime di sicurezza così come previste dall'art. 33 a 36 e all'allegato B (disciplinare tecnico) del d.lgs. 196/03, che, per quanto concerne il sistema informatico sono le seguenti:

- 1) **procedura di back up** dei dati al fine di garantire non solo l'integrità, ma anche la pronta disponibilità dei dati del Comune nei casi di realizzazione di una delle condizioni di cui sopra.
 - a. Per i computer che lavorano in rete il back up è effettuato **giornalmente** con salvataggio su uno dei due personal computer tramite hd esterno
 - b. Le copie di back up registrate devono essere conservate nell'archivio generale sotto la diretta responsabilità del responsabile del trattamento dati.

È noto che la copiatura di files su CD o DVD o dischi magneto-ottici non è sufficientemente sicura in quanto i supporti non sono adeguati per una conservazione stabile. Tuttavia i dati salvati su tali sistemi sono di importanza assolutamente secondaria e relativa e non possono dare luogo a conseguenze negative nell'assolvimento dei compiti istituzionali dell'Ente. Quindi, valutato il rapporto rischi/benefici, si ritiene valido anche questo sistema.
- 2) **Tutto il personale deve essere informato e formato** sui rischi e sulle misure di sicurezza, intendendo per queste, anche i comportamenti corretti che l'utente deve tenere. Qualora gli incaricati o i responsabili non rispettino le regole e le misure di sicurezza imposte col presente Documento Programmatico per la Sicurezza e le circolari interne distribuite e consegnate dal Comune medesimo, si applicheranno le sanzioni disciplinari come previsto dalla legge e dal contratto di lavoro.
- 3) Deve essere installato ed aggiornato uno specifico software antivirus in tutti i PC in dotazione al Comune. L'aggiornamento dell'antivirus è fatto automaticamente per tutti i computer. La scansione del computer con l'antivirus avviene almeno settimanalmente ed il controllo di tale operazione è affidata agli amministratori del sistema. Tali procedure di aggiornamento sono per la maggior parte automatizzate grazie al lavoro del server.. Il personale inoltre, è stato adeguatamente informato sui comportamenti corretti da tenere per evitare di introdurre virus informatici nel sistema.
- 4) Il personale è informato sul comportamento da seguire qualora utilizzi supporti rimovibili come floppy disk, chiavette hard disk, cd riscrivibili e non, etc...). Tutte le copie o i dati conservati nei supporti rimovibili devono essere conservati con cura, in luoghi adatti, lontani dalla portata delle persone non incaricate al trattamento di quei dati, tenendo tali supporti in cassette o armadi chiusi a chiave.
- 5) La manutenzione degli strumenti elettronici sia a livello hardware, che a livello software, qualora non sia possibile gestirla internamente viene affidata a società esterne appositamente scelte. Gli incarichi ed i relativi contratti saranno predisposti in modo da tenere conto delle esigenze previste nel presente DPS.
- 6) Sono impartite istruzioni specifiche agli incaricati al fine di non lasciare incustodite le stazioni di lavoro.
- 7) Le attività del Comune affidate alla gestione esterna non hanno una dichiarazione scritta che certifichi che siano state rispettate ed implementate le misure minime di sicurezza previste dal D.lgs. 196/03, ma il Comune entro la prossima revisione del

DPS si impegna ad ottenerla da tutte le imprese a cui sono e saranno affidati i lavori in *outsourcing*.

TABELLA 5: Le misure di sicurezza adottate o da adottare

Misura	Rischio contrastato	Trattamento interessato	Misura già in essere	Misura da adottare	Periodicità e responsabilità dei controlli
Copie di back up	Perdita dei dati, mal funzionamento, indisponibilità o degrado degli strumenti, sabotaggio del sistema, azioni di virus informatici, errori materiali dovuti alle più svariate cause, asportazione e furto degli strumenti contenenti dati, eventi distruttivi	Tutti i trattamenti svolti con l'ausilio di strumenti informatici che il Comune effettua.	Copie giornaliere su HD esterni		Amministratori del sistema, almeno una volta al mese.
Informazione e formazione del personale	Ridurre il più possibile i rischi derivanti da scarsa informazione ed errori umani	Tutti i trattamenti svolti con l'ausilio di strumenti informatici che il Comune effettua.	Tramite corsi specifici. Sono inoltre distribuite a tutto il personale Comune, circolari interne con i regolamenti da seguire relativi all'uso degli strumenti		Almeno annualmente devono effettuati dei corsi di aggiornamento e delle revisioni delle circolari. Sono incaricati a tali aggiornamenti gli

Documento programmatico per la sicurezza – Comune di Duno

			elettronici, supporti rimovibili, uso e custodia delle password....		amministratori del sistema.
Armadi chiusi a chiave e cassetti muniti di serratura	Al fine di evitare e ridurre il rischio di furti e trattamenti illecito ed indebito di dati da parte di chi non ne possiede l'autorizzazione	Tutti i trattamenti svolti con l'ausilio di strumenti informatici, sia per quanto riguarda la creazione di supporti necessari allo svolgimento del lavoro, sia per quanto concerne la creazione di copie.			Ciascun responsabile per il trattamento dei dati nelle varie aree del Comune effettua mensilmente controlli relativi all'osservazione di tali regole.
Antivirus	Al fine di evitare i danni derivanti dalle azioni di virus informatici e simili programmi "pirata".	Interessa tutti i computer in dotazione al Comune	Aggiornamento in automatico per tutti i computer.		Ogni volta che c'è un aggiornamento dell'antivirus vi è un controllo da parte dell'amministratore del sistema.
Credenziali di autenticazione e password	Al fine di evitare accessi abusivi e accessi non autorizzati	Interessa tutti i trattamenti che avvengono tramite supporto informatico	Accesso alla workstation tramite un profilo personalizzato per ogni utente e una		Il controllo periodico del cambio delle password è a carico dell'amministratore del sistema. Il

Documento programmatico per la sicurezza – Comune di Duno

			password da cambiare periodicamente.		responsabile del trattamento dei dati per ciascuna area collabora con l'amministratore del sistema per il controllo annuale dei profili di autenticazione adeguati alle mansioni di ciascun incaricato.

4.b DESCRIZIONE DEL SISTEMA DI ARCHIVIZIONE CARTACEA DEI DATI: ANALISI, RISCHI E MISURE DI SICUREZZA

Attualmente il sistema di archiviazione delle pratiche delle varie attività del Comune è manuale, basato su realizzazione e creazione di supporti cartacei. Permanendo tale organizzazione, dovrà essere supportata da un Archivio Generale.

Resteranno fuori da tale archivio le pratiche relative all'assistenza sociale (tutte chiuse negli armadi dell'ufficio dell'assistente sociale che rimane chiuso a chiave) e le pratiche relative all'Ufficio Anagrafe e Stato civile che resteranno nell'ufficio anagrafe.

Dopo una attenta analisi del tipo di trattamenti effettuati, si è giunti alla conclusione che non è possibile, sul piano pratico, distinguere i dati sensibili da quelli delle altre categorie. Infatti, pressoché in tutti i procedimenti trattati è possibile la presenza di documentazione contenente dati giudiziari o sensibili.

Pertanto, allo scopo di rispettare la normativa in materia, si è deciso di trattare e conservare l'intera mole della documentazione trattata dal Comune come dati sensibili, con esclusione di quelli conoscibili da pubblici elenchi o albi (ad es.: verbali e/o delibere del Consiglio Comunale, Delibere della Giunta Comunale, Albo Pretorio).

I rischi per i dati conservati nella forma del supporto cartaceo sono:

- perdita accidentale o deliberata;
- distruzione;
- incendio;
- allagamento;
- furto;
- accessi abusivi agli archivi di conservazione dei dati.

Le misure di sicurezza adottate per ridurre i rischi ai dati conservati in forma cartacea, ai sensi degli art. 31 e 33 e allegato B del D.lgs.vo 196/03, sono:

- conservazione dell'archivio contenente dati sensibili in armadio chiuso a chiave;
- archivio generale chiuso con serratura e custodia delle chiavi da parte dei responsabili del trattamento dei dati;
- consegna, a ciascun utente del Comune di Duno, di una circolare interna, la n. 3/P, contenente il "Regolamento di utilizzo degli archivi cartacei comunali";
- Identificazione e registrazione del personale che accede (anche con autorizzazione) agli archivi dopo l'orario di chiusura degli stessi, ai sensi della circolare interna n. 4/P.

Particolare attenzione deve essere prestata ai dati trattati dall'ufficio dell'assistente sociale che deve sempre chiudere a chiave la stanza dove sono ubicati gli archivi e il personal computer. La chiave la conserva l'incaricata stessa del trattamento e il responsabile dell'ufficio servizi alla persona.

La stessa attenzione va dedicata anche al registro del T.S.O. (trattamento sanitario obbligatorio). I dati devono essere conservati in un armadio chiuso a chiave, lontani da

luoghi accessibili al pubblico. Le chiavi devono essere custodite dal responsabile dell'ufficio polizia, incaricato al trattamento.

5.PROCEDURE DI BACK UP E RIPRISTINO DEI DATI

Il Comune d informa e forma tutto il suo personale sulle procedure di back up che obbligatoriamente saranno effettuate dagli amministratori del sistema e dagli incaricati del trattamento, una volta al giorno (da lunedì' al sabato) tramite registrazione dei dati su HD esterni di grandi dimensioni.

L'amministratore del sistema unitamente al responsabile per il trattamento dei dati di ciascuna area operativa controllano la giusta realizzazione delle copie di sicurezza, che dovranno essere riposte in luoghi fuori dall'accesso comune (come sale riunioni e corridoi) e conservate in archivi muniti di serratura.

Per i particolari, si veda il punto 1 del capitolo 4.a.

A tutto il personale del Comune è consegnata una circolare interna che descrive le procedure di back up e di ripristino dei dati.

Programmazione delle prove di ripristino dei dati.

Le procedure di ripristino sono uguali per ciascun settore di attività del Comune. Devono essere effettuate dal responsabile ed amministratore del sistema, ovvero sotto la sua diretta sorveglianza, nel minor tempo possibile e comunque in modo tale che non superi sette giorni per quanto riguarda i dati sensibili e giudiziari, così come prescritto dal disciplinare tecnico allegato al Codice della Privacy.

6. FORMAZIONE DEL PERSONALE

Il Comune riconoscendo l'importanza della formazione, in particolar modo riguardo alla tematica della sicurezza, e al fine di ridurre i rischi al proprio sistema informatico, s'impegna a promuovere momenti formativi.

In particolare, ai sensi del D.lgs.vo 196/03, tali verranno effettuati periodicamente ed in ogni caso al momento dell'entrata in servizio o al momento dei cambiamenti di mansioni o all'introduzione di nuovo strumenti elettronici che hanno impattato sul trattamento dei dati personali. Il Comune provvederà a chiedere un adeguato programma di formazione.

7. MODALITA' DI AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

Il titolare del trattamento è il soggetto preposto all'aggiornamento e alla custodia del documento programmatico per la sicurezza.

Il documento deve essere aggiornato ogni volta che vi sono cambiamenti significativi nello studio professionale impattanti sulle misure minime di sicurezza.

Il titolare del trattamento dovrà procedere alla completa revisione del documento in oggetto annualmente, salvo nuove e diverse indicazioni normative e/o disposizioni del garante.

Duno, 25.03.2011