Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

PULA SERVIZI E AMBIENTE

CODICE DELLA PRIVACY

(D.L.vo N. 196/2003)

DISPOSIZIONI MINIME SULLA SICUREZZA

E

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente documento si compone di n. 22 pagine (inclusa la presente) e allegati

Data di emissione: 10.12.2016

Il responsabile della sicurezza
Antonello Orru'

AO System & Software
Via Piroddi, 35 09048 Sinnai (CA)
p.iva 03428680924
c.f. RRONNL75A22B354C

(firma leggibile)

AO System & Software di Antonello Orru', p.iva 03428680924, via piroddi, 35 09048 Sinnai (CA) cell. 3477365191, fax +39178222476

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

INDICE

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

PREMESSA

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato dalla Pula Servizi e Ambiente S.R.L., previsti dal D.L.vo 30/06/2003 Num. 196 "Codice in materia di protezione dei dati personali".
Il presente documento è stato redatto da Antonello Orrù, in qualità di Amministratore di Sistema, che provvede a firmarlo in calce.
Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere corrette nel più breve tempo possibile.

NORMATIVA DI RIFERIMENTO

D.L.vo n. 196 del 30/06/2003;
Regolamento per l'utilizzo della rete.

DEFINIZIONI E RESPONSABILITÀ

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.
Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla

AO System & Software di Antonello Orru', p.iva 03428680924, via piroddi, 35 09048 Sinnai (CA) cell. 3477365191, fax +39178222476

sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

TITOLARE: il titolare del trattamento è figura non prevista e la titolarità è esercitata dal rappresentante legale, tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

TITOLARE, RESPONSABILI, INCARICATI

Titolare del trattamento: Dott. Sanna Fabio
Responsabile del trattamento dei dati: Dott. Sanna Fabio
Amministratore di Sistema: Antonello Orrù
Incaricati del trattamento dei dati: come da allegato 1
Custode delle password: figura non prevista

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

ANALISI DEI RISCHI

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.
L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;
- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
- DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
- DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
- DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

INDIVIDUAZIONE DELLE RISORSE DA PROTEGGERE

Le risorse da proteggere sono:

- personale;
- dati/informazioni;
- documenti cartacei;
- hardware;
- software;

Per ulteriori dettagli vedere gli Allegati 1 e 3.

INDIVIDUAZIONE DELLE MINACCE

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse.

RISCHI	DELIBERATO	ACCIDENTALE	AMBIENTALE
Terremoto			X
Inondazione	X	X	X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi	X		
Danno volontario	X		
Interruzione di corrente		X	
Interruzione di acqua	X		
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile	X	X	
Temperatura e umidità eccessive			X
Polvere			X
Radiazioni elettromagnetiche		X	
Scariche elettrostatiche		X	
Furto	X		
Uso non autorizzato dei supporti di memoria	X		
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Masquerading dell'identificativo dell'utente	X		
Uso illegale di software	X	X	
Software dannoso		X	
Esportazione/importazione illegale di software		X	
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		
Guasto tecnico di provider di rete		X	
Danni sulle linee		X	X
Errore di trasmissione		X	
Sovraccarico di traffico		X	X
Intercettazione (Eavesdropping)	X		
Infiltrazione nelle comunicazioni		X	
Analisi del traffico		X	
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X	X	
Ripudio		X	
Guasto dei servizi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente		X	X
Uso non corretto delle risorse	X	X	
Guasto software		X	X
Uso di software da parte di utenti non autorizzati		X	X
Uso di software in situazioni non autorizzate	X	X	

Per ulteriori dettagli delle minacce relative all'aspetto informatico vedere l'Allegato 2

INDIVIDUAZIONE DELLE VULNERABILITÀ

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nell'articolo 6.

CRITICITA'	FATTORE DI RISCHIO
Personal Computer non in dominio	MEDIO

Note:

All'interno dell'infrastruttura ICT della Pula Servizi e Ambiente soltanto 3 postazioni (quelle dell'area finanza) sono nel dominio del comune, in questo modo non si possono adottare le misure minime di sicurezza attraverso policy di gruppo.
Misure di sicurezza da adottare:

L'amministratore di Sistema provvederà a configurare le impostazione all'interno del dominio alla prima data utile.
Misure di sicurezza consigliate: installare un firewall o dispositivo per isolare le postazioni dalla rete comunale

CRITICITA'	FATTORE DI RISCHIO
Presenza di materiale cartaceo all'interno della sala tecnica	ALTO
Sala tecnica non chiusa	ALTO

Note:

Il server è virtualizzato e collocato in una postazione client, in quanto l'unità hardware che lo ospitava non è più disponibile per guasto grave. Esso è collocato nell'area amministrativa contabile
Misure di sicurezza da adottare:

Misure di sicurezza consigliate:

Si consiglia l'acquisto di una nuova macchina server e posizionare il server virtualizzato su questo.
Chiusura della stanza tecnica ed eliminazione di qualsiasi materiale cartaceo.

INDIVIDUAZIONE DELLE CONTROMISURE

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico;
- contromisure di carattere procedurale;
- contromisure di carattere elettronico/informatico.

CONTROMISURE DI CARATTERE FISICO

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
- i locali ad accesso controllato contenente i server di rete sono all'interno di aree sotto la responsabilità del titolare, Dott. Sanna Fabio, le singole postazioni vengono custodite dai singoli incaricati degli uffici;
- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti;
- i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite dal titolare, Dott. Sanna Fabio;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dei dipendenti della Pula Servizi e Ambiente
- i locali sono provvisti di sistema di allarme e di estintore.

CONTROMISURE DI CARATTERE PROCEDURALE

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- per l'ingresso ai locali ad accesso controllato è necessaria preventiva autorizzazione da parte del Responsabile del trattamento e successiva registrazione su apposito registro;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli allarmi e degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- i registri, contenenti dati comuni e particolari, durante l'orario di lavoro devono essere tenuti in custodia e affidati al responsabile di turno. Al termine dell'orario di lavoro vengono depositati e successivamente raccolti da un incaricato del trattamento e conservati in luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio dell'orario di lavoro.

CONTROMISURE DI CARATTERE ELETTRONICO/INFORMATICO

Vedere l'Allegato 3.

NORME PER IL PERSONALE

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete (Allegato 4).

INCIDENT RESPONSE E RIPRISTINO

Vedere l'Allegato 3

PIANO DI FORMAZIONE

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Le finalità della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

AGGIORNAMENTO DEL PIANO

Il presente piano è soggetto a revisione annua obbligatoria con scadenza entro il 31 marzo, ai sensi dell'art. 19 allegato B del D.L.vo 30/06/2003 Num. 196. Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- Modifiche all'assetto organizzativo della ditta ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- Danneggiamento o attacchi al patrimonio informativo della ditta tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

AO System & Software di Antonello Orru', p.iva 03428680924, via piroddi, 35 09048 Sinnai (CA) cell. 3477365191, fax +39178222476

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

Elenco Allegati costituenti parte integrante di questo documento

- Allegato 1 - elenco trattamenti dei dati
- Allegato 2 - minacce hardware, minacce rete, minacce dati trattati, minacce supporti
- Allegato 3 - misure di carattere elettronico/informatico, politiche di sicurezza, incident response e ripristino
- Allegato 4 - regolamento per l'utilizzo della rete
- Lettere di incarico per il trattamento dei dati
- Lettera di incarico per il responsabile del trattamento
- Lettera di incarico per l'amministratore di sistema

Il presente Documento Programmatico sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati.

Il redattore del documento
Antonello Orru

_____
(firma leggibile)

Nota: Fonti di documentazione
Il modello di documento programmatico sulla sicurezza è stato predisposto consultando le seguenti fonti:

- http://www.garanteprivacy.it
- "Sicurezza informatica" EUCIP IT Administrator – Modulo 5 Testo di riferimento per la certificazione EUCIP - McGraw Hill ISBN 88-3864333-4 Tabelle Minacce e vulnerabilità Cap. 1
- Il regolamento per l'utilizzo della rete è stato derivato dal documento CISEL 0203G286 – CISEL Centro Studi per gli Enti Locali – Maggioli

AO System & Software di Antonello Orru', p.iva 03428680924, via piroddi, 35 09048 Sinnai (CA) cell. 3477365191, fax +39178222476

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

ALLEGATO 1 – ANALISI PROPEDEUTICA DELLA SITUAZIONE ATTUALE DELL'ENTE

TABELLA 1 - ELENCO DEL PERSONALE INCARICATO AL TRATTAMENTO

	Area di Competenza e mansione	Cognome e Nome	codice fiscale	luogo di nascita	data di scadenza (contratto federambiente)
1	amministratore	Sanna Fabio	SNNFBA75H06G203S	RESPONSABILE DEL TRATTAMENTO	30/04/2019
2	direttore tecnico e responsabile tecnico 37/08	Quarantiello Fabrizio	QRNFRZ73L14H118M	INCARICATI DEL TRATTAMENTO	30/11/2016
3	capo cantiere e preposto d.lgs 81/08 - manutentore elettricista - RLS	Zucca Francesco	ZCCFNC54E14B354L	INCARICATI DEL TRATTAMENTO	indeterminato
4	operatore macchina movimento terra - autista	Lecca Mario	LCCMRA53M28H088R	INCARICATI DEL TRATTAMENTO	indeterminato
5	operatore macchina movimento terra - autista	Cabras Giovanni Piero	CBRGNN59S08H088L	INCARICATI DEL TRATTAMENTO	indeterminato
6	operatore macchine trattrici - autista - addetto alla segnaletica	Satta Luigi	STTLGU64A10H088S	INCARICATI DEL TRATTAMENTO	indeterminato
7	idraulico - manutentore caldaie - elettricista - addetto alla segnaletica	Deiana Paolo	DNEPLA61C25B354C	INCARICATI DEL TRATTAMENTO	indeterminato
8	operaio generico - addetto alla segnaletica	Murgia Roberto	MRGGPP65C15H088S	INCARICATI DEL TRATTAMENTO	indeterminato
9	muratore - operaio generico	Murgia Mario	MRGMRA53D22H088F	INCARICATI DEL TRATTAMENTO	indeterminato
10	operaio generico	Ruggeri Michele	RGGMHL52E04H088H	INCARICATI DEL TRATTAMENTO	indeterminato
11	necroforo - operaio generico	Urru Piero	RRUPRI62B13D333N	INCARICATI DEL TRATTAMENTO	indeterminato
12	impiegato amministrativo	Fantaci Dario	FNTDRA70S27G273U	INCARICATI DEL TRATTAMENTO	31/05/2017
13	impiegata amministrativa	Monica Brughitta	BRGMNC68P49B354J	INCARICATI DEL TRATTAMENTO	15/12/2016
14	impiegato amministrativo	Monni Giuseppe	MNNGPP80D01B354T	INCARICATI DEL TRATTAMENTO	15/12/2016
16	capo cantiere e preposto d.lgs 81/08	Saiu Corrado	SAICRD61B19H974W	INCARICATI DEL TRATTAMENTO	indeterminato
15	preposto d.lgs 81/08 - manutentore elettricista	Onnis Alberto	NNSLRT73E29B354B	INCARICATI DEL TRATTAMENTO	indeterminato
17	manutentore elettricista	Serra Riccardo	SRRRCR59B02H088I	INCARICATI DEL TRATTAMENTO	indeterminato
18	idraulico	Garau Salvatore	GRASVT70H28F979H	INCARICATI DEL TRATTAMENTO	indeterminato
19	idraulico e operaio generico	Urru Fabrizio	RRUFRZ78T19B354G	INCARICATI DEL TRATTAMENTO	indeterminato
20	giardiniere	Vargiu Sandro	VRGSDR73C01H088O	INCARICATI DEL TRATTAMENTO	indeterminato
21	operaio edile	Panduccio Severino	PNDSRN65T30B675G	INCARICATI DEL TRATTAMENTO	indeterminato
22	impiegata amministrativa	Balloi Patrizia	BLLPRZ72E50B354P	INCARICATI DEL TRATTAMENTO	31/12/2016

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

TABELLA 2 - ELENCO DELLE BANCHE DATI E DEI TRATTAMENTI

PR	S/N	TRATTAMENTO BANCA DATI	PERS	SENSIBILI GIUDIZIARI	CARTA	DIGITALE	ENTRAMBI	PC ISOLATO	PC RETE	A	B	C	D	E	F
		PAGHE E STIPENDI PERSONALE													
		PAGHE E STIPENDI CANTIERE													
		CERTIFICATI ASSENZA E MALATTIA													
		FASCICOLI DEL PERSONALE													
		RAPPORTI INAIL													
		RAPPORTI INPS													
		DELEGHE SINDACALI													
		CONTRATTI INDIVIDUALI DI LAVORO													
		PROVVEDIMENTI DI COLLOCAMENTO A RIPOSO													
		TRATTAMENTI PENSIONISTICI													
		BANCA DATI GESTIONE DEL PERSONALE (STIPENDI, CESSIONI DEL													
		QUINTO, DELEGHE SINDACALI, CERTIFICAZIONI DEI REDDITI)													
		BANCA DATI SISTEMA PREVIDENZIALE E ASSISTENZIALE													
		BANCA DATI FASCICOLI DEL PERSONALE													
		BANCA DATI RILEVAZIONE PRESENZE E GIUSTIFICATIVI ASSENZE													
		CREDITORI E DEBITORI													
		BANCA DATI AMMINISTRATORI													
		BANCA DATI CONCESSIONI DI BENEFICI ECONOMICI A PRIVATI E IMPRESE													

LEGGENDA

A = PORTA CHIUSA CON SERRATURA
B = ARMADIO CHIUSO CON SERRATURA
C = ARMADIO BLINDATO
D = SISTEMA DI AUTENTICAZIONE
E = SISTEMA DI PROTEZIONE AMBIENTALE
F = GRUPPO DI CONTINUITA'

E1=ANTIINCENDIO
E2=ANTIINTRUSIONE
E3=ANTIALLAGAMENTO
E4=RILEVAZIONE FUMI
E5= INFERRIATE ALLE FINESTRE

TABELLA 3 - ELENCO PERSONAL COMPUTER

NOME MACCHINA	SISTEMA OPERATIVO INSTALLATO	SOFTWARE UTILIZZATO	RETE	UFFICIO	INCARICATO	TIPI DI DATO

Tipi di Dato:

DA: DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DP: DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DS: DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

DG: DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

TABELLA 4 - CONNETTIVITÀ INTERNET

Connettività: ADSL ATTRAVERSO LA RETE LAN COMUNALE

Apparecchiature di comunicazione:

APPARECCHIATURA LOCALIZZAZIONE TIPOLOGIA

MODEM ROUTER FIRWALL JUNIPITER
Municipio ROUTER

Provider: TISCALI/TELECOM

ALLEGATO 2 – MINACCE

MINACCE A CUI SONO SOTTOPOSTE LE RISORSE HARDWARE

Le principali minacce alle risorse hardware sono:
- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;

MINACCE A CUI SONO SOTTOPOSTE LE RISORSE CONNESSE IN RETE
Le principali minacce alle risorse connesse in rete possono provenire dall'interno, dall'esterno o da una combinazione interno/esterno e sono relative:
All'utilizzo della LAN/Intranet (interne);
Ai punti di contatto con il mondo esterno attraverso Internet (esterne);
- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

In dettaglio si evidenziano le seguenti tecniche:
IP spoofing
L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.
Packet sniffing
Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso é possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.
Port scanning
Serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.
Highjacking
Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione é complessa e richiede elevate capacità e rapidità d'azione.
Social engineering
Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.
Buffer overflow
Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;
Spamming
Saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.

AO System & Software di Antonello Orru', p.iva 03428680924, via piroddi, 35 09048 Sinnai (CA) cell. 3477365191, fax +39178222476

Password cracking
Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.
Trojan
Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.
Worm
Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).
Logic bomb
Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.
Malware e MMC (Malicious Mobile Code)
Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.
DOS (Denial of Service)
Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.
DDOS (Distributed Denial of Service)
Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete

L'utilizzo di programmi di sniffing e port scanning è riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete locale LAN, tali programmi non sono in nessun caso utilizzati su reti esterne a quella della rete loca LAN.
La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dalla Autorità Giudiziaria.

Minacce a cui sono sottoposti i dati trattati
Le principali minacce ai dati trattati sono:
- accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

Minacce a cui sono sottoposti i supporti di memorizzazione
Le principali minacce ai supporti di memorizzazione sono:
- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

ALLEGATO 3 – MISURE, INCIDENT RESPONSE, RIPRISTINO

MISURE DI CARATTERE ELETTRONICO/INFORMATICO

Le misure di carattere elettronico/informatico adottate sono:

- utilizzo di server con configurazioni di ridondanza;
- presenza di gruppi di continuità elettrica per il server e per le singole postazioni informatiche;
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità settimanale e storico di un mese (MISURA IN FASE DI ATTIVAZIONE);
- installazione di un firewall software dedicato per proteggere la rete dagli accessi indesiderati attraverso internet;
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows (MISURA IN FASE DI ATTIVAZIONE);
- installazione di un sistema antivirus su tutte le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria;
- definizione delle regole per la gestione di strumenti elettronico/informatico (MISURA IN FASE DI ATTIVAZIONE);
- definizione delle regole di comportamento per minimizzare i rischi da virus (MISURA IN FASE DI ATTIVAZIONE).

REGOLE PER LA GESTIONE DELLE PASSWORD

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale.
User-id e password iniziali sono assegnati dall'Amministratore di Sistema.
User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.
La User-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.
La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.
Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.
Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.
Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.
In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:
Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
Per la definizione/gestione della password devono essere rispettate le seguenti regole:

- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere più di due caratteri identici consecutivi;
- non deve contenere lo user-id come parte della password;

AO System & Software di Antonello Orru', p.iva 03428680924, via piroddi, 35 09048 Sinnai (CA) cell. 3477365191, fax +391782224768

- al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
- la nuova password non deve essere simile alla password precedente;
- la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
- la password termina dopo sei mesi di inattività;
- la password è segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;
- l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia

REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICO/INFORMATICO

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- divieto di utilizzare floppy disk come mezzo per il backup;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- Divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- Limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, DOCX, XLS, XLSX;
- Controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- Evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di " scaricare "dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;
- Disattivare gli ActiveX e il download dei file per gli utenti del browser Internet Explorer;
- Disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);

- Attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- Non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- Non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
- Non utilizzare le chat;
- Consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- Non attivare le condivisioni dell'HD in scrittura.
- Seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- Avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- Conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- Conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- Conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- Conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

- Formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo. (Molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
- Installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
- Reinstallare i programmi applicativi a partire dai supporti originali;
- Effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
- Effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- Ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

INCIDENT RESPONSE E RIPRISTINO

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- Discrepanze nell'uso degli user-id;
- Modifica e sparizione di dati;
- Cattive prestazioni del sistema (così come percepite dagli utenti);
- Irregolarità nell'andamento del traffico;
- Irregolarità nei tempi di utilizzo del sistema;
- Quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. Evitare danni diretti alle persone;
2. Proteggere l'informazione sensibile o proprietaria;
3. Evitare danni economici;
4. Limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. Isolare l'area contenente il sistema oggetto dell'incidente;
2. Isolare il sistema compromesso dalla rete;
3. Spegnere correttamente il sistema oggetto dell'incidente (vedi tabella 3).

Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso;

4. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.

Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

- Eseguire una copia bit to bit degli hard disk del sistema compromesso;
- Se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
- Se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC (vedere Allegato 2) il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

AO System & Software di Antonello Orru', p.iva 03428680924, via piroddi, 35 09048 Sinnai (CA) cell. 3477365191, fax +39178222476

Tabella 3 - Procedure di spegnimento

Sistema operativo MS DOS

	Azione
1.	Fotografare lo schermo e documentare i programmi che sono attivi.
2.	Staccare la spina dalla presa di corrente.

Sistema operativo UNIX/Linux

	Azione
1.	Fotografare lo schermo e documentare i programmi che sono attivi.
2.	Se la password di root è disponibile eseguire il comando su e poi i comandi sync e halt.
3.	Se la password di root non è disponibile staccare la spina dalla presa di corrente.

Sistema operativo Mac

	Azione
1.	Fotografare lo schermo e documentare i programmi che sono attivi.
2.	Cliccare Special.
3.	Cliccare Shutdown.
4.	Una finestra indicherà che è possibile spegnere il sistema.
5.	Staccare la spina dalla presa di corrente.

Sistema operativo Microsoft Windows

	Azione
1.	Fotografare lo schermo e documentare i programmi che sono attivi.
2.	Staccare la spina dalla presa di corrente.

Nota: (fonte U.S. Department of Energy)

ALLEGATO 4 - REGOLAMENTO PER L'UTILIZZO DELLA RETE

OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

Il Pula Servizi e Ambiente promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.
Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.
Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.
Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

ABUSI E ATTIVITÀ VIETATE

E' vietato ogni tipo di abuso. In particolare è vietato:
- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile, come specificato nell'allegato 3.

ATTIVITÀ CONSENTITE

E' consentito all'amministratore di sistema:
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'allegato 3;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.
L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.
L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.
Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili, l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.
L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

MODALITÀ DI ACCESSO ALLA RETE E AGLI APPLICATIVI

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.
L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.
L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.
Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password e rispettare le norme indicate nell'allegato 3.

SANZIONI

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti interni