S.R.R. ATO N. 4
AGRIGENTO
Società per la Regolamentazione del servizio di gestione Rifiuti Agrigento Provincia Est

Sede legale: piazza Aldo Moro,1 92100 Agrigento
Tel. 0922 443011; Fax 0922 443019
Sito: **www.srrato4agest.it**

Uffici: piazza Trinacria zona industriale 92021 Aragona
Email: **info@srrato4agest.it** ; PEC: srrato4@legalmail.it

CODICE DELLA PRIVACY

(D.Lgs. n. 196/2003 e ss.mm.ii.)

DISPOSIZIONI MINIME SULLA SICUREZZA E PROGRAMMA DELLA SICUREZZA

Il presente documento si compone di n. 38 pagine (inclusa la presente)

Data di emissione:

L'Amministratore di Sistema

_____

(**Ing. Pierangelo Sanfilippo**)

Il Titolare del trattamento dei dati

_____

(**Vella Enrico**)

Indice

Denominazione Società

S.R.R. ATO n. 4 Agrigento Est

P.zza Trinacria, 1

92021 Aragona - Zona ASI AG

P.IVA 02734620848

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 S.R.R. ATO 4 Agrigento Est, previsti dal D.Lgs. 30/06/2003 N. 196 "Codice in materia di protezione dei dati personali".
Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Normativa di riferimento

D.Lgs. 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 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 Vella Enrico 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: Enrico Vella
Responsabili del trattamento dei dati:

- Dott. Guarneri Claudio
- Arch. Alletto Gaetano
- Dott.ssa Mendola Concetta Assunta
- Rag. Romito Giuseppe
- Geom. Traina Pasquale
- Ing. Sanfilippo Pierangelo
- Ing. Francesco Lazzaro
- Arch. Pietro Lucchesi

Amministratore di Sistema: Ing. Pierangelo Sanfilippo
Incaricati del trattamento dei dati: **come da allegato 1 - Nomine**

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		
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.

Infrastruttura	**Hardware**	**Comunicazioni**
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Locazione suscettibile ad allagamenti	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto

		Gestione inadeguata della rete
		Connessioni a linea pubblica non protette

Documenti cartacei	**Software**	**Personale**
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

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

- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti, le apparecchiature informatiche, gli archivi cartacei;
- i locali sono provvisti di estintore;
- i locali sono dotati di armadi ignifughi, impianti elettrici, sistemi di condizionamento, apparecchiature di continuità elettrica.

Contromisure di carattere procedurale

- i responsabili dei trattamenti devono mantenere un effettivo controllo sull'area di sua responsabilità;
- i visitatori occasionali sono accompagnati da un incaricato;
- l'ingresso ai locali 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;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli estintori;
- il responsabile del trattamento dei dati è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del responsabile del trattamento dei dati che è chiuso a chiave, una chiave di riserva è mantenuta con le dovute cautele dalla ditta ;
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato nella stanza protocollo

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.Lgs. 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.

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
- Lettere di incarico per i responsabili del trattamento
- Lettera di incarico per i custodi delle password
- Lettera di incarico per l'amministratore di sistema
- Lettere di riservatezza per gli addetti alle pulizie

L'Amministratore di Sistema

_____

(**Ing. Pierangelo Sanfilippo**)

ALLEGATO 1 – Elenco trattamenti dei dati

Tabella 1 - Elenco dei trattamenti dei dati

Finalità perseguita o attività svolta	Categorie di interessati	Natura dei dati trattati	Struttura di riferimento	Altre strutture che concorrono al trattamento	Descrizione degli strumenti utilizzati
Attività di Segreteria	Enti, Enti Soci ed utenti	Dati Personali semplici	Affari Generali e segreteria amministrativa	Ufficio amministrazione, gestione e formazione del personale	PC. desktop collegati in rete ed a internet Armadi
Gestione della contabilità aziendale	Enti Soci, Banche, Clienti e Fornitori	Dati Personali semplici	Ufficio Contabilità	Affari Generali e segreteria amministrativa	PC. desktop collegati in rete ed a internet Armadi
Gestione degli acquisti in economia	Fornitori	Dati Personali semplici	Ufficio di Tesoreria ed economato	Ufficio Contabilità	PC. desktop collegati in rete ed a internet Armadi
Controllo di gestione della Società	Enti, Enti Soci, Società di revisione dei bilanci e Revisori dei conti	Dati Personali semplici	Ufficio Auditing e Controllo di Gestione	Ufficio Contabilità	PC. desktop collegati in rete ed a internet Armadi
Gestione della TARSU e della TIA	Utenti	Dati Personali semplici	Ufficio Elaborazione TIA-TARSU	Affari Generali e segreteria amministrativa	PC. desktop collegati in rete ed a internet Armadi
Controllo e verifica delle denunce della TARSU e della TIA	Utenti	Dati Personali semplici	Ufficio ispettivo, controllo e verifica denunce	Ufficio Elaborazione TIA-TARSU	PC. desktop collegati in rete ed a internet Armadi
Attività di accertamento della TARSU e della TIA	Utenti	Dati Personali semplici	Ufficio Evasione ed Elusione	Ufficio Elaborazione TIA-TARSU	PC. desktop collegati in rete ed a internet Armadi
Gestione della riscossione TARSU e TIA	Enti, Enti Soci ed Utenti	Dati Personali semplici	Ufficio Riscossione	Ufficio Elaborazione TIA-TARSU	PC. desktop collegati in rete ed a internet Armadi

Relazioni con il pubblico	Enti Soci ed utenti	Dati Personali semplici	Ufficio relazione con il pubblico	Affari Generali e segreteria amministrativa	PC. desktop collegati in rete ed a internet Armadi
Gestione dei servizi di igiene ambientale	Enti, Enti Soci ed utenti	Dati Personali semplici	Ufficio per l'attuazione del contratto di servizio	Ufficio amministrazione, gestione e formazione del personale	PC. desktop collegati in rete ed a internet Armadi
Attività di pianificazione e per l'accesso ai finanziamenti	Enti, Enti Soci	Dati Personali semplici	Ufficio Progettazione, Pianificazione e Finanziamenti.	Affari Generali e segreteria amministrativa	PC. desktop collegati in rete ed a internet Armadi
Gestione dei CCR e delle Isole ecologiche	Enti Soci, utenti	Dati Personali semplici	Ufficio CCR, Isole Ecologiche e Formulari	Ufficio amministrazione, gestione e formazione del personale	PC. desktop collegati in rete ed a internet, totem e portatili non collegati in rete Armadi
Gestione del parco automezzi della Società	Assicurazioni, officine	Dati Personali semplici	Ufficio Manutenzione e Gestione Automezzi	Ufficio amministrazione, gestione e formazione del personale	PC. desktop collegati in rete ed a internet Armadi
Gestione del personale	Dipendenti	Dati Personali semplici e sensibili	Ufficio amministrazione, gestione e formazione del personale	Ufficio Contabilità	PC. desktop collegati in rete ed a internet Armadi
Gestione delle attrezzature informatiche	Dipendenti	Dati Personali semplici	Ufficio CED	Ufficio CED	PC. desktop collegati in rete ed a internet Armadi

Tabella 2 - Descrizione della struttura organizzativa

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Segreteria Organi e Rapporti con Istituzioni	Gestione della posta e delle comunicazioni cartacee.	Acquisizione e caricamento, anche mediante il protocollo informatico, delle comunicazioni e della posta. Consultazione del protocollo e delle comunicazioni archiviate. Redazione, trasmissione ed archiviazione delle comunicazioni.
Ufficio Contabilità e Bilancio	Gestione della contabilità della Società. Gestione delle piccole spese societarie.	Registrazione ed archiviazione delle fatture ricevute dai fornitori. Elaborazione e trasmissione di fatture Vs. clienti. Predisposizione del bilancio Societario. Gestione delle fatture delle piccole spese della Società. Verifiche della cassa relativa all'economato.
Ufficio Auditing e Controllo di Gestione	Sistema di Controllo aziendale.	Rapporti con le Società di revisione del bilancio. Rapporti con i revisori. Verifiche di cassa. Verifiche della fatturazione.
Ufficio Elaborazione TIA-TARSU	Gestione delle denunce dei contribuenti ai fini TARSU e TIA	Registrazione delle pratiche dei contribuenti. Aggiornamento dei database TARSU e TIA
Ufficio ispettivo, controllo e verifica denunce	Gestione delle pratiche TARSU e TIA.	Controllo e verifica denunce TARSU e TIA.
Ufficio Evasione ed Elusione	Gestione delle pratiche relative all'evasione ed elusione ai fini TARSU e TIA	Incrocio di database per l'emersione dell'evasione e dell'elusione. Invio di accertamenti ai contribuenti. Gestione degli accertamenti relative ad omesse denunce ed infedeli denunce. Front office con gli utenti.
Ufficio Riscossione	Gestione della riscossione delle bollette TARSU e TIA.	Emissione bollette TARSU e TIA. Gestione delle pratiche TARSU e TIA.
Ufficio relazione con il pubblico	Front office per informazioni agli utenti.	Consultazione delle istanze degli utenti. Risoluzione delle problematiche poste dagli utenti.
Ufficio per l'attuazione del contratto di servizio	Gestione dei servizi di igiene urbana espletati nei Comuni Soci.	Gestione del personale che effettua i servizi di igiene urbana comandati presso le ditte di servizio. Gestione del personale che effettua la gestione diretta nei Comuni Soci. Gestione dei contratti di servizio.
Ufficio Progettazione, Pianificazione e Finanziamenti.	Progettazione e pianificazione di servizi e dell'impiantistica della Società.	Progettazione e pianificazione di servizi e dell'impiantistica. Acquisizione dei dati del personale impiegato nei servizi di igiene urbana nei Comuni Soci finalizzati alla progettazione ed alla pianificazione dei Servizi di igiene urbana.

Ufficio CCR, Isole Ecologiche e Formulari	Gestione delle attività dei CCR e delle Isole Ecologiche.	Gestione del personale impiegato nei CCR e nelle isole ecologiche. Redazione dei formulari per il conferimento presso gli impianti autorizzati dei rifiuti urbani differenziati e/o speciali. Gestione delle isole ecologiche e dei CCR di proprietà della Società.
Ufficio Manutenzione e Gestione Automezzi	Gestione degli automezzi aziendali	Manutenzione ordinaria e straordinaria degli automezzi aziendali. Gestione delle assicurazioni.
Ufficio amministrazione, gestione e formazione del personale	Gestione del personale dipendente della Società.	Gestione assenze/presenze. Acquisizione dei certificati medici dal sito INPS. Registrazione dei permessi e delle malattie. Gestione delle pratiche per infortunio sul lavoro. Formazione del personale. Gestione delle visite mediche periodiche. Cura degli adempimenti previsti per il personale aziendale.
Ufficio CED	Gestione delle infrastrutture informatiche aziendali.	Gestione delle manutenzione su software e hardware aziendale. Coordinamento dei salvataggi dei dati. Creazione di nuove infrastrutture informatiche.

Tabella 3 - Elenco del personale incaricato del trattamento in ogni struttura e delle dotazioni informatiche.

Cognome e Nome	Struttura di riferimento	Strumenti utilizzati	Responsabilità aggiuntive
Mendola Concetta Assunta	Ufficio Tributi	Utente-Pc: - CLONE PC - Dual core - Win 7 - Hd da 500 Gb - KAV 2012	Responsabile del trattamento dei dati
Pinto Loredana	Segreteria Organi e Rapporti con Istituzioni	PINTO: DMOUMGJ 72df3d2c-6c19-49f2-a13a-55coab97953b - Win 10 pro - Hd da 800 Gb	
Romito Giuseppe	Ufficio Contabilità e Bilancio	GIUSEPPE: - dual core - Win X8 - Hd da 1 Gb	Responsabile del trattamento dei dati
Castronovo Giuseppe	Ufficio ARO Palma di Montechiaro	solea-E-1456895C: - CLONE PC - Dual core - Win Xp - Hd da 300 Gb	
Curreri Calogero	Ufficio Contabilità e Bilancio	Lillo: - dual core - Win X8 - Hd da 500 Gb	
Di Giacomo Giuseppa	Ufficio Tributi	SECONDO: - CLONE PC - Dual cp serie 55274-648-0846111-23739 - Win XP/2002 - Hd da 1,00 Gb	
GESA- Argento Onofrio	Ufficio Tributi	pentium 76435-OEM-0052016-47447 -HD 2,00 GB di Ram - Win XP intel®	

Zammito Giuseppa	Ufficio Tributi	- CLONE PC - Pentiun 4 - Win Xp - Hd da 300 Gb	
Bellomo Domenica	Ufficio Tributi	Pentium ® 2.80GHz - Dual core CPU E6300 - Win XP 2,00 Gb di Ram	
La Porta Salvatore	Controllo e Monitoraggio	- Olidata - Pentium 4 - Win Xp - Hd da 300 Gb	
Guarneri Claudio	Direttore Generale	Intel core i7-7700 cpu @ 3600 GHZ Win 10	Responsabile del trattamento dei dati
Traina Pasquale	Ufficio Supporto ARO	Intel Core i7 7100 - Wind 10 - Hd da 930 4B	Responsabile del trattamento dei dati
Danile Nicodemo	Ufficio APEA	- CLONE PC - Pentium 4 - Win Xp - Hd da 80 Gb	
Scrudato Michele	Ufficio Tributi	Utente-Pc: 16,0 GB di Ram Intel ® Core ™ -I7-6700 - Win 7	
Lattuca Alfonso	Ufficio Tributi	00371-OEM-9044301-10660 Sistema operativo 64 bit Intel®- Celeron	

		- Win 7 4,00 Gb di Ram	
Bonvissuto Carmelo	Piani Operativi di Finanziamento	Intel® 76435-OEM-0048995-61330 - Win XP - Hd da 1,99 Gb di Ram	
Maglio Gerlando	Ufficio Tributi	- CLONE PC - Dual core - Win XP - Hd da 320 Gb	
Graci Vincenzo	ARO c/o SRR	PC versione 2002 Intel-Pentium® 4 CPU 1,75 Gb di Ram 76435-OEM-0061626-73888	
Terrana Enzo Antonio	Ufficio Tributi	- CLONE PC - Dual core - Win Xp 2.00 GHz, 0,99Gb di ram	
Aleo Eleonora	Ufficio APEA	Pc-Eleonora: - Windows 10	
Di Rosa Salvatore	Ufficio Reclami	PC versione 2002 Intel-Pentium® 4 CPU 1,75 Gb di Ram 76435-OEM-0061626-73888	
Bonvissuto Carmelo	Piani operativi di Finanziamento	PINTO: - ASUS - Pentium 4 - Win xp - Hd da 300 Gb	
Vizzì Giuseppe	Ufficio Tributi	numero serie 00371-oem-8992671-00004 -Intel® - Windows-7 - Hd da 1.80 Gb	
Amato Pietro	Ufficio APEA	Windows 10	

Lombardo Sergio	Ufficio Controllo e Monitoraggio	- CLONE PC - Dual core - Win Xp - Hd da 300 Gb	
Arceri Concetta	Uffio Tributi	-Pc: 55274-6404237903-23565 -Dual Core Xp -Hd da 500 Pentium	
Alletto Gaetano	Ufficio Impianti	Intel Core i7 7100 Hd da 930 4b Win 10	Responsabile del trattamento dei dati
Petix Matteo	Ufficio Tributi	-Dual Core -Pentium -Win Xp	
Mondello Nunzio Alfonso	Ufficio Segreteria e Rapporti con istituzioni	- CLONE PC - Dual core - Win Xp - Hd da 300 Gb	
Sciarrabone Vito	Ufficio CCR, Isole Ecologiche e Formulari	ESE 0009 - Q.re Fontanelle: - ASEM - Pentium 3 - Win Xp - Hd da 20 Gb	
Vetro Carmelo	Ufficio Aro c/o SRR	Win xp – versione 2002 Intel- Pentium® 3,40 GHz	Manutenzione attrezzature CCR ed isole ecologiche
Cilia Vincenzo	Ufficio Contabilità e bilancio	PC- dual core -Win X8 -Hd 10 pro	
Caramanno Giovanni	Ufficio CCR, Isole Ecologiche e Formulari	CAM 0071 - mTOT 0072 - Mobile: - ASEM - Pentium 3 - Win Xp - Hd da 20 Gb	

Licata Angelo	Ufficio CCR, Isole Ecologiche e Formulari	CAM 0056 - TOTEM 0108 - Racalmuto: - ASEM - Pentium 3 - Win Xp - Hd da 20 Gb	CCR di Racalmuto
Tornabene Salvatore	Ufficio CCR, Isole Ecologiche e Formulari	CAM 0056 - TOTEM 0108 - Racalmuto: - ASEM - Pentium 3 - Win Xp - Hd da 20 Gb	CCR Racalmuto –
Maggio Emanuele DITTA	Ufficio CCR, Isole Ecologiche e Formulari	CCA 0059 - Raffadali: - ASEM - Pentium 3 - Win Xp - Hd da 20 Gb	
Graceffa Giuseppa	Ufficio CCR, Isole Ecologiche e Formulari	Utente Pc: - ACER - Dual core - Win 7 - Hd da 250 Gb	'Isola ecologica di Aragona
Iacono Salvatore	Ufficio CCR, Isole Ecologiche e Formulari	ESE 0011 - P.za Ugo La Malfa: - ASEM - Pentium 3 - Win Xp - Hd da 20 Gb	CCR di Agrigento
Campione Antonio	Piano D'Ambito e Collegamento Piano Regionale	Pc-Utente: - AMD Semperon - Win 7 - Hd da 22 Gb	
Castellana Lucia Rosalia	Ufficio Risorse Umane	Olidata Pentium D Hd da 160 Gb	
Mirabile Gianfranco	Ufficio Attrezzature e Automezzi	Versione 2002 - CLONE PC - INTEL ® Core 2 duo 76435-OEM-0045813-46894 - 3.00GHz 3.50 GB di Ram	

Ing. Pierangelo Sanfilippo	Ufficio Controllo e Monitoraggio	Intel core i7-7700 cpu @ 3600 GHZ Hd da 1000 Gb Win 10	Responsabile del trattamento dei dati
Petix Cristina	Ufficio CED-Pricacy- Gare e contratti	- PC versione 2002 - Win Xp - Hd da 1 di ram	

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.

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 é 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

Tabella 1 - Connettività internet

Connettività	Apparecchiature di comunicazione	Provider
ADSL	Router	Fastweb
ADSL	Router	Telecom Italia

Tabella 2 - Descrizione Personal Computer

Identificatico del PC	Tipo PC	Sistema operativo	Software utilizzato	Rete
Sanfilippo Pierangelo	Intel core i7-7700 cpu @ 3600 GHZ Hd da 1000 Gb	Win 10	Office 2016 HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Danil - Danile	CLONE PC Pentium 4 Hd da 80 Gb	Win XP	Collegamento Serpico Open Office 4.1.4 serpico HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Amato		Win 10	Open - Office HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Traina	Intel Core i7 7100 - Wind 10 - Hd da 930 4B	Win 10	SICRA HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Utente-Pc - Scrudato	Utente-Pc: 16,0 GB di Ram Intel ® Core ™ -I7-6700 - Win 7	Win 7	Serpico Suite (collegamento Serpico e rendicontazione) Office 2010 HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Alfonso-Pc - Lattuca	00371-OEM-9044301-10660 Sistema operativo 64 bit Intel®- Celeron - Win 7 4,00 Gb di Ram	Win 7	Serpico Suite (collegamento Serpico e rendicontazione) Office 2007 HALLEY 2006 (collegamento Protocollo e portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
– Di Giacomo	- CLONE PC	Win XP	Serpico (collegamento Serpico e rendicontazione)	Alla rete aziendale - connessione ad internet tramite

	- Dual cp serie 55274-648-0846111-23739 - Win XP/2002 - Hd da 1,00 Gb		Arianna Gefil HALLEY 2006 (collegamento portale del dipendente)	rete aziendale
gesa1 - Argento	pentium 76435-OEM-0052016-47447 -HD 2,00 GB di Ram - Win XP intel®	Win XP	Serpico Suite (collegamento Serpico e rendicontazione) Gefil HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Bellomo	Pentium ® 2.80GHz - Dual core CPU E6300 2,00 Gb di Ram	Win XP	Serpico Gefil Office 2007 HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Salvatore La Porta	Hd da 320 Gb	Win XP	Office 2007 SICRA HALLEY 2006	
E - Cuffaro	CLONE PC Dual core Hd da 300 Gb	Win XP		
Enzo - Terrana	Intel pentium Dual core 2.00 GHz 0.99 Gb	Win XP	Collegamento Serpico Arianna HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Pc-Eleonora - Aleo	Olidata	Win 10	Collegamento Serpico Open Office Autolado 2010 HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Pc-Utente - Campione	CLONE PC AMD Semperon Hd da 22 Gb	Win 7	Halley rss Office 2010 HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale

Alletto - Alletto	Olidata Pentium 4 Hd da 930 4b	Win XP	Office 4.1.4 HALLEY rss (collegamento portale del dipendente) Aruba mail	Alla rete aziendale - connessione ad internet tramite rete aziendale
Mondello	- Win 10 pro - Hd da 800 Gb		Archidò Office 2007 HALLEY 2006 (collegamento protocollo e portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Graci Vincenzo	PC versione 2002 Intel-Pentium® 4 CPU 1,75 Gb di Ram 76435-OEM-0061626-73888	Win XP	Office 2007 HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Lillo - Curreri	CLONE PC Dual core -Hd 500 Gb	Win X8	Office - Teamsystem HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
GIUSEPPE - Romito	CLONE PC Dual Core Hd da 1 Gb	Win X8	Office - Teamsystem HALLEY 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Castellana	Olidata Pentium D Hd da 160 Gb	Win XP	Office 2007 MySQL-Front Pegaso HALLEY 2006 (collegamento presenze e portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Pc14 - Mirabile	CLONE PC Core 2 duo Hd da 500 Gb	Win XP	Office 2007 Collegamento Serpico Procedura Halley 2006 Halley 2006 (collegamento portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
PINTO - Pinto	DMOUMGJ 72df3d2c-6c19-49f2-a13a-55coab97953b - Win 10 pro - Hd da 800 Gb	Win XP	Archidò Office 2007 HALLEY 2006 (collegamento protocollo e portale del dipendente)	Alla rete aziendale - connessione ad internet tramite rete aziendale
Utente-Pc - Mendola	Dual core	Win 7	Serpico Suite (collegamento Serpico e rendicontazione) Office 2007	Alla rete aziendale - connessione ad internet tramite rete aziendale

	Hd da 500 Gb		HALLEY 2006 (collegamento portale del dipendente)	
Guarneri	Intel core i7-7700 cpu @ 3600 GHZ	Win 10	Office 2010 Collegamento Serpico HALLEY 2006 (collegamento presenze e portale del dipendente) Teamportal SICRA	Alla rete aziendale - connessione ad internet tramite rete aziendale
ESE 0009-Q.re Fontanelle	ASEM Pentium III Hd da 20 Gb	Win XP	IDEA BS-DATA6.9	
ESE 0010 - V.ggio Peruzzo	ASEM Pentium III Hd da 20 Gb	Win XP	IDEA BS-DATA6.9	
ESE 0011-P.za Ugo La Malf	ASEM Pentium III Hd da 20 Gb	Win XP	IDEA BS-DATA6.9	
ESE 0012 - Via Imera	ASEM Pentium III Hd da 20 Gb Pentium III Hd da 20 Gb Pentium III Hd da 20 Gb	Win XP	IDEA BS-DATA6.9	
CCA 0059 - Raffadali	ASEM Pentium III Hd da 20 Gb Pentium III	Win XP	IDEA BS-DATA6.9	
Utente Pc - Isola Aragona	ACER Dual core Hd da 250 Gb Dual core Hd da 250 Gb	Win 7	Office 2007	

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;
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità settimanale e storico di un mese.
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows XP , 7, 10;
- installazione di un sistema antivirus (Kaspersky, Avast varie versioni) su tutte le postazioni di lavoro, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria.

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 state assegnate. User-id e password sono strettamente personali.
La password è composta da caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore ed è stata 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 Nome e Cognome e\o eventualmente 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 disattivate dopo tre mesi di non utilizzo.
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 occorrerà 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 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;
- al primo accesso la password ottenuta dal custode delle password è stata 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;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup sono realizzate sui NAS
- 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 fax si trova in locale ad accesso controllato (stanza protocollo) e l'utilizzo è consentito unicamente agli incaricati del trattamento (sig.ra Loredana Pinto)

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, chiavette usb) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;*
- *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 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;

Tabella 3 - Procedure di spegnimento

Sistema operativo	Azione
MS DOS	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.
UNIX/Linux	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.
Mac	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.
Windows 98/NT/2000/XP/10	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.

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

La S.R.R. ATO 4 Agrigento Est promuove l'utilizzo della rete quale strumento utile per 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. L'utente e gli operatori hanno 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.

L'Amministratore di Sistema	Il Titolare del trattamento dei dati
_____	_____
(**Ing. Pierangelo sanfilippo**)	(Enrico Vella)