

TERIACA TRAVEL POINT

in attuazione del

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

GDPR

Il presente documento si compone di n. 23 pagine (inclusa la presente)

Data di emissione: 20/05/2018

Il responsabile della sicurezza

(firma leggibile)

TERIACA TRAVEL POINT di L. Teriaca

Via Etnea 245-247
95030 Mascalucia CT

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 protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati effettuato da TERIACA TRAVEL POINT di L. Teriaca, in ottemperanza al REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016.

Il presente documento è stato redatto da Dott.ssa Lidia Concetta Teriaca. in qualità di Titolare - Direttore Tecnico, che provvede a firmarlo in calce.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Normativa di riferimento

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Definizioni e responsabilità

- 1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- 2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- 4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- 5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- 6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- 7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- 8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- 9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- 10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- 11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- 12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- 13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- 14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- 15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione

ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (1);

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Altre definizioni

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.

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.

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, responsabili, incaricati

Titolare del trattamento: Dott.ssa Teriaca Lidia Concetta

Responsabile del trattamento dei dati: Dott.ssa Lidia Concetta Teriaca

Responsabile della sicurezza informatica: Dott.ssa Lidia Concetta Teriaca

Amministratore della rete: figura non prevista

Custode delle password: Dott.ssa Lidia Concetta Teriaca

Incaricati del trattamento dei dati: come da allegato 1

Incaricato dell'assistenza e della manutenzione degli strumenti elettronici: figura non prevista

DPO: figura no prevista

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

- 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 sono all'interno di aree sotto la responsabilità della Dott.ssa Lidia Teriaca
- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità della Dott.ssa Lidia Concetta Teriaca
- 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 agli incaricati del trattamento ovvero gli impiegati;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- non sono previsti visitatori occasionali delle aree ad accesso controllato;
- 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 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;

Contromisure di carattere elettronico/informatico

Vedere l'Allegato 3.

Norme per il personale

Tutti i dipendenti concorrono alla realizzazione della sicurezza ed alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, 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 in accordo alle disposizioni previste dal regolamento e dalle direttive a riguardo ed in ogni caso 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
- Lettera di incarico per il responsabile del trattamento
- Lettera di incarico per il custode delle password
- Lettera di incarico per l'amministratore di sistema

Il presente Documento Programmatico è divulgato e illustrato a tutti gli incaricati.

Il redattore del documento

(firma leggibile)

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
Gestione pratiche viaggio	Clienti	Dati Personali semplici	Booking	Gestione Pratiche	PC, internet e moduli cartacei laddove previsto
Gestione Amministrativa pratiche viaggio	clienti, fornitori, servizi	Dati Personali semplici	Amministrazione	Gestione Pratiche	PC, internet e moduli cartacei laddove previsto

Finalità perseguita o attività svolta: menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es. gestione del personale, gestione collaboratori, gestioni clienti, gestioni fornitori, ecc.) e delle **categorie di persone** cui i dati si riferiscono (personale, collaboratori, clienti, fornitori, ecc.).

Natura dei dati trattati: indicare la classe di rischio dei dati trattati tenendo presente la seguente classificazione:

- 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.

Struttura di riferimento: indicare la struttura (segreteria amministrativa, direzione, funzione svolta, ecc.) all'interno della quale viene effettuato il trattamento.

Altre strutture che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture è opportuno indicare, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.

Descrizione degli strumenti utilizzati: va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi) e altre tipologie di contenitori (es. armadi, schedari...).

Tabella 2 - Descrizione della struttura organizzativa

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Booking	Trattamento dei dati anagrafici necessari alla prenotazione dei servizi richiesti sia nelle piattaforme degli operatori che in quella della stessa organizzazione.	Accettazione clienti; preventivi, prenotazione servizi, emissione e consegna documenti di viaggio.
Gestione Pratiche	Trattamento dati anagrafici e propri dei servizi richiesti e contrattualizzazione della prenotazione degli stessi	Immissione e modifica dati sulle piattaforme di prenotazione e su quella proprietari
Amministrazione	Trattamento dati anagrafici, dati propri dei servizi richiesti e dati contabili	Utilizzo dati per emissione e richiesta Estratti conto e fatture

Struttura: riportare le indicazioni delle strutture menzionate nella Tabella 1.

Trattamenti effettuati dalla struttura: indicare i trattamenti di competenza di ciascuna struttura.

Compiti e responsabilità della struttura: descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.).

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
Dimartino Simona	Booking	PC, Internet e laddove previsto moduli cartacei	
Abate Martina	Gestione Pratiche	PC, Internet e moduli cartacei laddove previsto	
Dott.ssa Teriaca Lidia Concetta	Amministrazione	PC, Internet moduli cartacei laddove previsto	
Dott.ssa Lidia Concetta Teriaca	Booking	PC, internet e moduli cartacei laddove previsto	

Nome e cognome: riportare le indicazioni per ogni incaricato del trattamento.

Struttura di riferimento: riportare l'indicazione della struttura di appartenenza di ogni incaricato.

Strumenti utilizzati: per ogni incaricato riportare le informazioni relative allo strumento utilizzato (p.e. numero di inventario del PC).

Responsabilità aggiuntive: indicare le eventuali responsabilità aggiuntive rispetto all'incarico per il trattamento dei dati, ad esempio "responsabile del trattamento", "responsabile delle copie di backup", "custode delle chiavi di un contenitore o armadio", "custode delle password", ecc.

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 è 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 è 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 Ethernet fornito dall'operatore telefonico dotato di firewall; nessun DMZ configurato;	Wind - infostrada

Connettività: indicare il tipo di connettività internet (XDSL, ISDN, PSTN).

Apparecchiature di comunicazione: indicare il tipo di apparecchiature utilizzate per la connettività (modem, router).

Provider: indicare il fornitore di connettività.

Tabella 2 - Descrizione Personal Computer

Identificativo del PC	Tipo PC	Sistema operativo	Software utilizzato	Rete
pc01	Portatile Sony Vaio	Windows 7	Client Posta elettronica, Browser Web, Software terminale CRS, OpenOffice, Adobe Acrobat Reader, driver e utility standard	Ethernet classica filare
pc02	Lenovo i5 portatile	Windows 7	Client Posta elettronica, Browser Web, Software terminale CRS, OpenOffice, Adobe Acrobat Reader, driver e utility standard	Ethernet standard filare
pc03	Toshiba portatile	Windows 7	Client Posta elettronica, Browser Web, OpenOffice, Adobe Acrobat Reader, driver e utility standard; server e client per la gestione della biglietteria spettacoli, Ricezione FAX	Ethernet Standard filare
pc04	Asus portatile	Windows 8	Client Posta elettronica, Browser Web, Software terminale CRS, OpenOffice, Adobe Acrobat Reader, driver e utility standard; server piattaforma proprietaria con db proprietario	Ethernet standard filare

Identificativo del PC: indicare l'elenco di tutti i PC utilizzati sia connessi che non connessi alla rete (per esempio con il numero di inventario).

Tipo PC: indicare il tipo del PC.

Sistema operativo: indicare quale Sistema operativo è utilizzato sul PC.

Software utilizzato: indicare il software applicativo utilizzato per il lavoro (es. OFFICE, STAROFFICE, ecc...).

Rete: indicare se il PC è connesso alla rete.

Misure di carattere elettronico/informatico

Le misure di carattere elettronico/informatico adottate sono:

- Copie di back su server remoto con periodicità giornaliera
- La continuità elettrica sui pc tutti è assicurata dalla natura portatile dei pc che includono pertanto batteria.
- definizione delle regole per la gestione delle password;
- 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. (da adottare entro la fine dell'anno)

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, dal custode delle password.

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;
- 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;
- gli hard disk condivisi in rete sono quelli che non contengono dati sensibili relativi alle attività di vendita ;
- 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 realizzate su ...(indicare il dispositivo, CD, cassetta, ecc...) sono conservate in...(specificare il tipo di contenitore es. armadio chiuso a chiave , e indicare la sua ubicazione)
- 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 (specificare dove) e l'utilizzo è consentito unicamente agli incaricati del trattamento (specificare chi)

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, 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 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 reinstallare il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
- installare il software antivirus, verificare 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 prestare 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 riaccessato;
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.

Tabella 3 - Procedure di spegnimento

Sistema operativo	Azione
MS DOS	<ol style="list-style-type: none">1. Fotografare lo schermo e documentare i programmi che sono attivi.2. Staccare la spina dalla presa di corrente.
UNIX/Linux	<ol style="list-style-type: none">3. 1. Fotografare lo schermo e documentare i programmi che sono attivi.4. Se la password di root è disponibile eseguire il comando su e poi i comandi sync e halt.5. Se la password di root non è disponibile staccare la spina dalla presa di corrente.
Mac	<ol style="list-style-type: none">6. 1. Fotografare lo schermo e documentare i programmi che sono attivi.7. Cliccare Special.8. Cliccare Shutdown.9. Una finestra indicherà che è possibile spegnere il sistema.10. Staccare la spina dalla presa di corrente.
Windows 98/NT/2000/XP	<ol style="list-style-type: none">11. 1. Fotografare lo schermo e documentare i programmi che sono attivi.12. 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

TERIACA TRAVEL POINT di L. Teriaca 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 distruggano 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.