Direzione: DIREZIONE

Delibera del Presidente (con Firma Digitale)

N. **D00028** **del** **14/08/2020** **Proposta n.** 234 **del** 14/08/2020

Oggetto:

Adempimenti ex regolamento (UE) 2016/679. Adozione del disciplinare per l'utilizzo delle postazioni di lavoro, dei servizi di rete, della posta elettronica e di internet per il trattamento dei dati personali della RISERVA NATURALE REGIONALE MONTE NAVEGNA E MONTE CERVIA.

Estensore
CARLONI VINCENZO
_____firma elettronica_____

Responsabile del Procedimento
LODOVISI VINCENZO
_____firma elettronica_____

Il Direttore
V. LODOVISI
_____firma digitale_____

Il Presidente
G. RICCI
_____firma digitale_____

Richiesta di pubblicazione sul BUR: NO

IL PRESIDENTE

Assunti i poteri del Consiglio

VISTA la Legge Regionale n° 56 del 09/09/1988 istitutiva di questa Riserva Naturale;

VISTA la Legge Regionale 22 maggio 1995, n. 29, avente ad oggetto "Modifiche ed integrazioni leggi regionali in attuazione all'art. 13 della legge regionale 18 novembre 1991, n. 74 (Disposizioni in materia di tutele ambientale – Modifiche ed integrazioni alla legge regionale 11 aprile 1985, n. 36);

VISTA la Legge 6 dicembre 1991, n. 394 "Legge Quadro sulle Aree Protette";

VISTA la Legge Regionale 6 ottobre 1997, n. 29, "Norme in materia di aree naturali protette regionali" e successive modificazioni;

VISTO l'art. 9 della Legge Statutaria Regionale 11 novembre 2004, n. 1, di approvazione del "Nuovo Statuto della Regione Lazio";

VISTA altresì, la Legge Regionale14 luglio 2014 n° 7, che all'art. 1 stabilisce funzioni e compiti degli organi di controllo degli enti pubblici dipendenti della Regione Lazio;

VISTA la Legge Regionale 20 novembre 2001 n. 25, "Norme in materia di programmazione, bilancio e contabilità della regione", che definisce al Titolo VII, Capo I, artt. 56-60, la disciplina normativa da applicare agli Enti Pubblici dipendenti dalla Regione Lazio in materia di bilanci e rendiconti;

VISTO il Decreto del Presidente della Regione Lazio n° T00287 del 23/11/2018 di nomina del Presidente dell'Ente Regionale "Riserva Naturale Regionale Monte Navegna e Monte Cervia" nella persona del Sig. Giuseppe Ricci;

VISTO il Decreto del Presidente della Regione Lazio n° T00018 del 15/01/2020 di nomina del Direttore della Riserva Naturale Monte Navegna e Monte Cervia nella persona del Dott. Vincenzo Lodovisi;

VISTO il contratto di diritto privato per il conferimento dell'incarico di Direttore del Parco, sottoscritto tra il Presidente e il Dott. Vincenzo Lodovisi in data 03/02/2020;

VISTO il Decreto del Presidente della Regione Lazio n. T00094 dell' 8 giugno 2020, avente ad oggetto "Nomina Revisore dei conti unico e Revisore dei conti supplente della RNR Monte Navegna e Monte Cervia di cui all'art.15 della L.R. 6 ottobre 1997 n. 29, così come modificato dall'articolo 2, comma 15, lettera b), della legge regionale 14 luglio 2014, n. 7" con il quale è stato nominato Revisore dei conti unico dell'Ente il Dott. Luca Cervelli e Revisore dei conti supplente il dott. Mario Galasso;

VISTA la deliberazione del Presidente dell'Ente n. 21 del 24/09/2019, di adozione dello schema di Bilancio di previsione triennale 2020-2022 con i relativi allegati;

VISTA la legge regionale 18 febbraio 2002, n. 6, recante disposizioni concernenti la "Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza ed al personale regionale" e successive modificazioni;

VISTO il Regolamento regionale 6 settembre 2002, n. 1 "Regolamento di organizzazione degli uffici e dei servizi della giunta regionale" e successive modifiche;

VISTI:

- Il 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);

- la legge 25 ottobre 2017, n. 163 (Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017) e, in particolare, l'articolo 13, ai sensi del quale il Governo è delegato all'adozione di uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento;

- la "Rettifica 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)"

- Il DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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)", che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679;

- La Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n.2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)";

- La Deliberazione del Garante per la protezione dei dati personali n. 13 del 1 Marzo 2007 "Le Linee guida del Garante per posta elettronica e internet";

- La normativa in materia di diritto d'autore e di altri diritti connessi al suo esercizio introdotta con la Legge n.633/41 per la protezione delle opere dell'ingegno di carattere creativo qualunque ne sia il modo o la forma di espressione;

- La normativa in materia di protezione del software introdotta con il D.Lgs. n.518/92 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori"; tale provvedimento normativo ha infatti aggiunto l'art. 171-bis, avente ad oggetto la tutela di programmi per elaboratori, all'art.171 della Legge n° 633/1941. L'art. 171-bis, il cui testo e stato ultimamente modificato dalla L. n° 248/2000 "Nuove norme di tutela del diritto d'autore", prevede sanzioni penali a carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di copyright; pertanto la norma pone il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuarne delle copie;

- La Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori);

- La Costituzione della Repubblica Italiana, art. 15 sancisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge";

- Il Codice Penale art. 616 - Violazione, sottrazione e soppressione di corrispondenza – "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o

sopprime, è punito, se il fatto non e previsto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, e punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto e punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per corrispondenza si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza;

VISTA la Deliberazione del Presidente dell'Ente n. D00026 del 12/08/2020 avente ad oggetto "Adozione del modello organizzativo in materia di titolarità, responsabilità del trattamento e protezione dei dati personali della RNR Monte Navegna e monte Cervia."

CONSIDERATO in particolare, il principio di "responsabilizzazione" ("accountability") che attribuisce, al titolare del trattamento, il compito di mettere in atto "misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento", alla luce "della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1. del RGPD);

PRESO ALTRESÌ ATTO della necessità di rivedere lo stesso regolamento alla luce della nuova normativa in materia di privacy su richiamata nonché delle linee di indirizzo dettate dal Garante;

VISTO lo schema di regolamento per l'utilizzo delle postazioni di lavoro, dei servizi di rete, della posta elettronica e di internet per il personale autorizzato al trattamento dei dati dell'Ente, predisposto dagli uffici;

ATTESO CHE il Direttore dell'Ente ha espresso, in merito alla presente deliberazione, parere favorevole in ordine alla regolarità tecnico-amministrativa;

DELIBERA

per i motivi espressi in premessa, che costituiscono parte integrante e sostanziale della presente deliberazione:

1. di adottare il regolamento per l'utilizzo delle postazioni di lavoro, dei servizi di rete, della posta elettronica e di internet per il personale autorizzato al trattamento dei dati dell'Ente RNR Monte Navegna e Monte Cervia allegato sotto la lettera A alla presente deliberazione, della quale costituisce parte integrante e sostanziale;

2. di trasmettere lo stesso al Direttore dell'Ente per gli atti conseguenti.

3. di disporre la pubblicazione del presente atto sul sito internet istituzionale nella sezione Amministrazione Trasparente, sotto sezione "Altri contenuti - Accessibilità e Catalogo di dati, metadati e banche dati" e sotto sezione "Provvedimenti".

REGOLAMENTO PER L'UTILIZZO DELLE POSTAZIONI DI LAVORO, DEI SERVIZI DI RETE, DELLA POSTA ELETTRONICA E DI INTERNET PER IL PERSONALE AUTORIZZATO AL TRATTAMENTO DI DATI DELL'ENTE

TITOLO I– DISPOSIZIONI COMUNI E PRINCIPI GENERALI

TITOLO I – DISPOSIZIONI COMUNI E PRINCIPI GENERALI

ARTICOLO 1 - RIFERIMENTI NORMATIVI

Il presente Regolamento e stato redatto in ottemperanza a quanto disposto dalle norme sotto riportate:

- 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);

- DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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)", che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679;

- Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n.2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)";

- Deliberazione del Garante per la protezione dei dati personali n. 13 del 1 Marzo 2007 "Le Linee guida del Garante per posta elettronica e internet";

- Normativa in materia di diritto d'autore e di altri diritti connessi al suo esercizio introdotta con la Legge n.633/41 per la protezione delle opere dell'ingegno di carattere creativo qualunque ne sia il modo o la forma di espressione;

- Normativa in materia di protezione del software introdotta con il D.Lgs. n.518/92 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori"; tale provvedimento normativo ha infatti aggiunto l'art. 171-bis, avente ad oggetto la tutela di programmi per elaboratori, all'art.171 della Legge n° 633/1941. L'art. 171-bis, il cui testo e stato ultimamente modificato dalla L. n° 248/2000 "Nuove norme di tutela del diritto d'autore", prevede sanzioni penali a carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di copyright; pertanto la norma pone il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuarne delle copie;

- Legge 20 maggio 1970, n. 300 "Norme sulla tutela della liberta e dignità dei lavoratori, della liberta sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori);

- Costituzione della Repubblica Italiana, art. 15 sancisce che "La liberta e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge";

- Codice Penale art. 616 - Violazione, sottrazione e soppressione di corrispondenza – "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, e punito, se il fatto non e preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, e punito, se dal fatto deriva nocumento ed il fatto medesimo non

costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto e punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per ≪corrispondenza≫ si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza;

ARTICOLO 2 - FINALITÀ

Il presente Regolamento:

- norma l'utilizzo delle postazioni di lavoro, dei servizi di rete, della posta elettronica e di internet da parte dei dipendenti dell'Ente Monti Cimini Riserva Naturale Lago di Vico (di seguito Parco) nonché da parte dei soggetti che, a qualunque titolo (collaboratori, stagisti, tirocinanti ecc.) accedono al "Sistema Informativo del Parco" (di seguito SIP) siano individuati quali autorizzati al trattamento di dati personali ai sensi dell'art. 29 del GDPR n. 2016/679/UE;

- detta le misure di sicurezza per la protezione dei dati personali da applicare nel caso di operazioni effettuate su archivi elettronici/cartacei cosi come discendenti dall'art. art. 32 del GDPR n. 2016/679/UE, che ciascun autorizzato al trattamento dati e chiamato ad adottare per dare piena applicazione a quanto disposto dalla normativa di settore. L'utilizzo dei beni e dei servizi resi disponibili dal SIP è svolto nel pieno rispetto delle norme del presente Regolamento al fine di non incorrere in responsabilità di ogni ordine e grado. Gli autorizzati al trattamento di dati personali non possono intraprendere attività non contemplate nel presente Regolamento in assenza di specifico assenso alle operazioni reso dal Responsabile del CED al fine di garantire che tali attività non contrastino con gli standard di sicurezza informatica stabiliti dall'Ente.

ARTICOLO 3 - DEFINIZIONI

Ai fini del presente Regolamento si intende per:

1.Account

Un account costituisce quell'insieme di funzionalità, strumenti e contenuti attribuiti ad un utente in determinati contesti operativi. In informatica, attraverso il meccanismo dell'account, il sistema mette a disposizione dell'utente un ambiente con contenuti e funzionalità personalizzabili, oltre ad un conveniente grado di isolamento dalle altre utenze parallele.

Infatti, il sistema e in grado di riconoscere l'identità del titolare di account, ne memorizza e conserva un insieme di dati ed informazioni attribuite ad esso, che possono essere gestite solo da lui e rimangono accessibili per un utilizzo futuro.

In questo si differenzia da altre modalità di accesso a sistemi di servizio interattivi che non presuppongono la ripetizione del rapporto con l'utente.

2.Amministratore di sistema

In ambito informatico sono le figure professionali finalizzate alla gestione e/o manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente atto sono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

3.Antivirus

Software che cerca ed elimina eventuali programmi virus rimediando ai danni provocati dal virus.

4.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.

5.Attachment/Allegato di posta elettronica

File o Documento di qualunque genere agganciato ad un messaggio di posta elettronica.

6.Autorizzati al Trattamento

Persone fisiche, espressamente designate, cui sono attribuiti specifici compiti e funzioni connessi al trattamento di dati personali sotto la diretta autorità del titolare o del responsabile. Ai fini del seguente documento si veda anche la definizione di Utente.

7.Backup

L'operazione tesa a duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita (per esempio una volta al giorno o alla settimana).

L'operazione di backup consente di recuperare i dati dell'utente o degli utenti che utilizzano la postazione; in caso di server o di database, tale recupero e essenziale per il lavoro di diverse persone.

8.Browser

Un browser web (in italiano: navigatore) e un programma che consente agli utenti di visualizzare e interagire con testi, immagini e altre informazioni, tipicamente contenute nella pagina web di un sito (o all'interno di una rete locale). (Es. Google Chrome)

9.Chat (webchat)

Sistema che consente il dialogo (tramite digitazione sulla tastiera) di più utenti contemporaneamente tramite Internet.

10.Client

In informatica, con client (in italiano detto anche cliente) si indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware o al software.

Un esempio di client hardware e rappresentato da un computer collegato, tramite una rete informatica (locale o geografica), ad un server al quale richiede uno o più servizi, utilizzando uno o più protocolli di rete.

Il termine client indica anche il software usato sul computer per accedere alle funzionalità offerte dal server.

11.Client di posta elettronica

Software che, collegandosi ad un server, consente lo scambio di messaggi e di file attraverso il servizio di posta elettronica. Il client standard all'interno del SIP e attualmente Microsoft Outlook.

12.Codice in materia di protezione dei dati personali

DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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)".

13.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;

14.Database (Base di Dati)

Qualsiasi aggregato di dati organizzato in campi (colonne) e record (righe).

15.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.

16.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.

17.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.

18.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.

19.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 e conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

20.Download

La registrazione su un supporto di registrazione (es. disco rigido del PC, Key USB, hard disc esterno) di un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).

21.E-mail

La E-Mail (abbreviazione di Electronic Mail, in italiano: posta elettronica) e un servizio internet grazie al quale ogni utente può inviare o ricevere dei messaggi.

22.Firewall

Una combinazione di hardware e software per garantire la sicurezza in una rete di computer proteggendola da accessi esterni non voluti. Con tale termine di origine inglese (significato originario: parete refrattaria, muro tagliafuoco) si fa riferimento al componente passivo di difesa perimetrale che può anche svolgere funzioni di collegamento tra due o più tronconi di rete.

23.Hardware

Con hardware, in ingegneria elettronica e informatica si indica la parte fisica di un personal computer, ovvero tutte quelle parti magnetiche, ottiche, meccaniche ed elettroniche che ne consentono il funzionamento (dette anche strumentario). Più in generale il termine si riferisce a qualsiasi componente fisico di una periferica o di una apparecchiatura elettronica.

24.Internet

Il termine internet ha al giorno d'oggi più significati, strettamente collegati, ma utilizzati in contesti differenti: il nome proprio "Internet" (scritto con l'iniziale maiuscola in quanto nome proprio ma anche con l'iniziale minuscola in quanto ormai ampiamente diffuso nel linguaggio comune) si riferisce alla prima ed unica rete di computer mondiale ad accesso pubblico realizzata. Il sostantivo comune internet (con la i minuscola) designa nella grande maggioranza dei casi l'accesso alla rete, vista pero questa volta come uno dei principali mezzi di comunicazione di massa, insieme con l'informazione e con i servizi che sono offerti agli utilizzatori per mezzo di questa rete. Dal punto di vista tecnico, inoltre, il termine può designare anche una rete di grandi dimensioni che interconnette delle reti autonome.

25.Intranet

L'intranet e una rete locale (LAN), o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l'accesso all'informazione, che può essere ad accesso ristretto. Rete locale che, pur non essendo necessariamente accessibile dall'esterno, fa uso di tecnologie Internet.

26.LAN (Local Area Network)

Una rete locale, in lingua inglese Local Area Network, in sigla LAN, e una tipologia di rete informatica contraddistinta da un'estensione territoriale limitata a qualche chilometro. L'implementazione classica di LAN e quella che serve un'abitazione o un'azienda all'interno di un edificio, o al massimo più edifici adiacenti fra loro al fine di non ricorrere a servizi di trasmissione dati esterni.

27.Limitazione di trattamento

Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

28.Mailing list

La Mailing-list (letteralmente, lista per corrispondenza, dalla lingua inglese; traducibile in italiano con lista di diffusione) e un sistema organizzato per la partecipazione di più persone in una discussione asincrona tramite email.

29.Password

Sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica (sportello bancomat, computer, connessione internet, casella email, reti, programmi, basi dati, ecc.) o per effettuare operazioni di cifratura.

Una password e solitamente associata ad uno specifico username (in italiano nome utente o identificatore utente) al fine di ottenere un'identificazione univoca da parte del sistema a cui si richiede l'accesso.

30.Postazioni di lavoro

Con il termine postazione di lavoro si intende l'insieme delle componenti hardware e software in dotazione ad un utente in virtù del suo ruolo e delle sue funzioni.

31.Plug-in

Con tale termini ci si riferisce ad un programma non autonomo che interagisce con un altro programma per ampliarne le funzioni. Il tipico esempio e rappresentato da un plug-in per un software di grafica che permette l'utilizzo di nuove funzioni non presenti nel software principale.

La capacita di un software di supportare i plug-in e generalmente un'ottima caratteristica, perché rende possibile l'ampliamento e la personalizzazione delle sue funzioni in maniera semplice e veloce.

32.Policy

Con tale termine si identificano le regole stabilite su un Server affinché tutte le workstation collegate siano "controllate" nello stesso modo e affinché su di esse siano presenti le stesse caratteristiche. Ogni buon amministratore di sistema dovrebbe utilizzarle.

33.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.

34.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.

35.Regolamento generale sulla protezione dei dati (GDPR 2016/679/UE)

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.

36.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.

37.Server

Un server (detto in italiano anche servente o serviente) e una componente informatica che fornisce servizi ad altre componenti (tipicamente chiamate client) attraverso una rete. Si noti che il termine server, cosi come pure il termine client, possono essere riferiti sia alla componente software che alla componente hardware.

38.SInfP - Sistema informatico del Parco

Con questo termine si intende l'insieme degli strumenti messi a disposizione al fine di poter accedere alle informazioni gestite dal sistema informativo dell'Ente RISERVA NATURALE REGIONALE MONTE NAVEGNA E MONTE CERVIA (di seguito denominato SIP).

Gli strumenti messi a disposizione appartengono a due tipologie:

-hardware (es. linee di connessione, monitor, personal computer, stampanti, server);

-software (es. programma di videoscrittura, applicazione per la gestione della contabilità).

39.Unità ICT

Unità operativa del Parco dedicata alla gestione della sicurezza informatica del Sistema Informatico dell'Ente

40.Software

Si intende ogni programma o applicazione informatica resa disponibile nell'ambito del SIP agli utenti.

41.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 autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

42.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.

43.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.

44.UserId

Nome utente

45.Utente

Ogni persona fisica che, in qualità di autorizzato al trattamento di dati personali, utilizza uno o più componenti del SInfP e che fruisce delle informazioni disponibili all'interno del SIP. La fruizione può essere piena come per tutti i dipendenti del Parco o soggetta a limitazioni come nel caso di soggetti esterni che svolgono per il Parco compiti contrattualmente definiti.

46.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.

47.Virus

Un virus e un software, appartenente alla categoria dei malware, che e in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di se stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano uno spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.

TITOLO II – ISTRUZIONI E NORME DI CONDOTTA PER IL PERSONALE AUTORIZZATO AL TRATTAMENTO DI DATI PERSONALI

ARTICOLO 4 - REGOLE DI ORDINARIA DILIGENZA

I soggetti autorizzati all'accesso al Sistema Informativo del Parco (di seguito SIP) nella fruizione di beni, servizi e informazioni resi disponibili dal SIP osservano l'obbligo di ordinaria diligenza, cosi come previsto dal Codice di comportamento dei dipendenti pubblici (D.P.R. 16 aprile 2013, n. 62) e dal Codice di comportamento del Parco.

In particolare l'autorizzato al trattamento, nell'esecuzione dei compiti assegnati, oltre ad attenersi alle regole di ordinaria diligenza al fine di evitare che soggetti estranei vengano a conoscenza dei dati personali oggetto del trattamento, e tenuto a:

- non divulgare a terzi estranei le informazioni di cui viene a conoscenza;

- non fare copie, per uso personale, dei dati su cui svolge operazioni;

- attenersi scrupolosamente alle istruzioni scritte;

- non trascrivere dati personali su fogli, agendine, post-it facilmente accessibili da terzi;

- in caso di abbandono temporaneo (per un periodo superiore a 15 minuti) della postazione di lavoro (scrivania, sportello, archivio):

  - chiudere gli eventuali archivi contenenti dati personali;
  - raccogliere la documentazione cartacea contenente dati personali in modo da non renderla visibile a terzi estranei al trattamento.

CAPO I - GESTIONE DEI DATI PERSONALI SU SUPPORTI NON AUTOMATIZZATI

ARTICOLO 5 - ARCHIVI SU SUPPORTI NON AUTOMATIZZATI

Tutti i dati personali presenti su supporti di tipo cartaceo, laddove possibile e compatibilmente con la dislocazione degli spazi, devono essere riposti in archivi mantenuti chiusi e dislocati all'interno di locali appositi con accesso controllato e limitato (con questo terminologia ci si riferisce ad aree o singoli uffici cui si accede previo accordo con il personale e sempre in presenza del personale addetto all'area o all'ufficio stesso).

Gli autorizzati al trattamento accedono unicamente agli archivi di propria competenza (ad es. solo quelli dell'unita organizzativa nella quale prestano la propria attività di lavoro) e adottano le seguenti norme di comportamento:

- limitano l'accesso all'archivio al tempo strettamente necessario allo svolgimento delle proprie mansioni;

- ripongono la documentazione prelevata dall'archivio al termine delle operazioni di trattamento. Nel caso in cui per esigenze di lavoro sia necessario mantenere per più giorni il possesso della documentazione, la persona autorizzata avrà cura di tenerli occultati alla vista di terzi estranei al trattamento;

- ripongono, una volta terminato il trattamento e comunque a fine giornata lavorativa, tutti i documenti contenenti dati sensibili e/o giudiziari in contenitori e/o locali muniti di serratura.

ARTICOLO 6 - RIPRODUZIONE DI DOCUMENTI CONTENENTI DATI PERSONALI (MEZZI DI TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Nell'utilizzo di fax, stampanti, fotocopiatrici, al fine di prevenire rischi di accesso ai dati non autorizzati, sono adottate opportune cautele nella trasmissione e riproduzione dei documenti.

A tal fine ciascun autorizzato al trattamento e tenuto a:

- non lasciare incustoditi presso fax, stampanti di rete o macchine fotocopiatrici al piano documenti contenenti dati personali;

- accertarsi dopo l'utilizzo della fotocopiatrice/fax/stampanti che non rimangano in macchina originali o copie contenenti dati personali. In caso di cattiva qualità della stampa distruggere il supporto cartaceo contenente dati personali e non riutilizzarlo come carta da riciclo ;

- nel caso di trasmissione via fax di documenti contenenti dati personali, avvertire telefonicamente il destinatario del documento e accertarsi dell'avvenuta ricezione. Una volta inviati i documenti, ritirarli immediatamente dalla macchina;

- accertarsi, nel caso di riproduzione/stampa di documenti contenente dati sensibili/giudiziari, che il contenuto di tali documenti non sia accessibile a soggetti estranei al trattamento;

CAPO II – HARDWARE E SOFTWARE

ARTICOLO 7 - BUONE NORME DI UTILIZZO DELLE RISORSE INFORMATICHE ASSEGNATE

All'utente autorizzato all'accesso, per esigenze di servizio, possono essere affidate in uso risorse informatiche come personal computer, computer portatili, tablet, smartphone, programmi e/o applicazioni che possono essere esclusivamente utilizzate per le attività istituzionali: non è assolutamente consentito l'uso per fini personali.

In tal caso ciascun soggetto autorizzato e tenuto a:

- custodire tali risorse in modo appropriato;

- utilizzare tali risorse limitatamente allo svolgimento delle attività lavorative loro assegnate;

- non utilizzare tali risorse per scopi illeciti;

- mettere in atto tutte le precauzioni necessarie al fine di evitare l'utilizzo della risorsa, e dunque l'accesso ai dati personali in essa contenuti, da parte di soggetti non autorizzati (es. predisposizione procedure di blocco del computer, attivazione screen saver, spegnimento del computer terminata la propria prestazione lavorativa).

In particolare si ricorda che sono tassativamente vietate le seguenti attività:

- utilizzare a titolo personale la posta elettronica assegnata;

- accedere a siti ed acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;

- diffondere prodotti informativi lesivi dell'onorabilità, individuali e collettivi;

- diffondere prodotti informativi di natura politica al di fuori di quelli consentiti dalla legge e dai regolamenti;

- diffondere, in rete o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura;

- compiere attività che compromettono in qualsiasi modo la sicurezza delle risorse informatiche e della rete del Titolare;

- compiere attività che possono rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, CD audio e video, clonazione o programmazione di smart card;

- utilizzare strumenti che potenzialmente sono in grado di consentire l'accesso non autorizzato alle risorse

informatiche (ad es. cracker, programmi di condivisione quali IRC, …);

- intraprendere azioni allo scopo di :

  - degradare le risorse del sistema;
  - ottenere risorse superiori a quelle già allocate ed autorizzate;
  - accedere a risorse informatiche, sia dell'Ente che di terze parti,violandone le misure di sicurezza;
  - svelare le password altrui, nonché trasmettere in chiaro, pubblicare o mandare in stampa liste di account utenti o nomi host e corrispondenti indirizzi IP delle macchine;

- impedire ad utenti autorizzati l'accesso alle risorse;

- utilizzare software di monitoraggio della rete in genere;

- intercettare pacchetti sulla rete, utilizzare sniffer o software di analisi del traffico (spyware) dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'utente oppure a controllare ogni attività, ivi inclusa la corrispondenza e i dati personali, dei dipendente;

- utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente;

- accedere ai locali e ai box riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi;

- installare hub per sottoreti di PC e stampanti;

- installare modem per chiamate su linee analogiche, digitali o xDSL;

- installare modem configurati in call-back ;

- accedere ai file di configurazione del sistema, farne delle copie e trasmetterle ad altri.

L'utilizzo di risorse informatiche private (notebook, tablet, smartphone, periferiche etc.) deve essere autorizzata dall' ICT, rispettando quanto prescritto relativamente alle configurazioni di sistema e al rispetto delle misure minime di sicurezza.

ARTICOLO 8 - LA POSTAZIONE DI LAVORO

Ogni persona autorizzata accede alla propria postazione di lavoro a lui assegnata in modo univoco, utilizzando la medesima:

- unicamente per lo svolgimento delle attività lavorative assegnate;

- laddove possibile, in modo esclusivo;

- avvalendosi esclusivamente del software fornito/approvato dal Parco;

- custodendola con diligenza.

Una postazione di lavoro può assumere le seguenti configurazioni:

- fissa, ovvero utilizzabile solo se connessa fisicamente alla rete del Parco;

- mobile, ovvero utilizzabile anche in altri luoghi.

Le funzioni/ i compiti svolti da ciascun soggetto autorizzato determinano la configurazione e le caratteristiche delle componenti delle postazioni di lavoro.

Una postazione di lavoro fissa e costituita generalmente da:

- monitor

- personal computer

- periferica di puntamento connessa con cavo (o wireless) al personal computer

- tastiera connessa con cavo (o wireless).

Una postazione di lavoro mobile può essere costituita da uno o più dei seguenti

- componenti:

- telefono cellulare

- tablet

- computer portatile e relativi dispositivi di connettività

- stampante portatile

Ciascun soggetto autorizzato e titolare di un'unica postazione di lavoro. Eventuali combinazioni con postazioni di lavoro mobili sono autorizzate in ottemperanza alle norme regolamentari dell'Ente.

Le caratteristiche della postazione di lavoro sono determinate dalle applicazioni fruibili dalla postazione di lavoro e sono suscettibili di adeguamenti sulla base dell'evoluzione tecnologica. Eventuali adeguamenti sono proposti dall' ICT.

In entrambe le tipologie di postazioni di lavoro il software applicativo installato e quello strettamente necessario a garantire l'espletamento delle funzioni/compiti di lavoro assegnategli.

L'utilizzo di più postazioni di lavoro e formalmente autorizzato dal Responsabile dell'ICT su richiesta del Dirigente/Responsabile del trattamento interessato, e validato dallo stesso o suo delegato per quanto attiene agli aspetti tecnici di sicurezza informatica, i servizi e le applicazioni utilizzabili da ciascuna postazione di lavoro in relazione alla configurazione del sistema informativo.

ARTICOLO 9 - CONFIGURAZIONE DELLA POSTAZIONE DI LAVORO

Nelle postazioni di lavoro sono installate applicazioni e resi disponibili servizi compatibili con la configurazione del sistema informativo della Riserva Naturale Regionale .

Nelle postazioni di lavoro sono installati unicamente i programmi necessari all'attività di ufficio di cui l'Ente detiene regolare licenza d'uso.

I soggetti autorizzati non sono configurati come amministratori del proprio computer, fatte salve casi eccezionali giustificati dalle mansioni lavorative e previa autorizzazione formale del Responsabile dell' ICT.

La configurazione di rete della propria postazione di lavoro può essere modificata solo dall'Amministratore di sistema a fronte di una formale autorizzazione da inoltrare all'ICT il quale, preso atto delle motivazioni della richiesta, si farà carico di dare seguito alla richiesta secondo un ordine di priorità calcolato sulla base del livello di criticità e delle altre attività contingenti.

Al fine di assicurare il corretto funzionamento del sistema ciascuna persona autorizzata e tenuta a:

- non modificare le configurazioni impostate sul proprio PC;

- non rimuovere o modificare, senza preventiva autorizzazione, alcun dato o apparecchiatura di proprietà della Riserva;

- non installare o configurare sul proprio PC mezzi di comunicazione o altre periferiche, senza preventiva autorizzazione (ad es. modem, masterizzatori, lettori MP3 o DVD, ecc.) da parte dell'Amministratore del sistema;

- non installare o utilizzare software non autorizzati preventivamente dal Parco e validati dall'Amministratore del sistema;

- non utilizzare software ricevuto in uso dal Parco per finalità extra lavorative;

- non distribuire, anche via e-mail, software potenzialmente dannoso per le risorse informatiche (in particolare tutti i programmi per l'apertura di eseguibili) del proprio PC;

- non utilizzare supporti di memorizzazione (ad es. cd rom, dvd, chiavi USB) di incerta provenienza senza la preventiva autorizzazione dell'Amministratore del sistema.

In linea generale ciascun soggetto autorizzato e tenuto ad adottare ogni opportuna cautela atta ad evitare danni, temporanei o permanenti, a sistemi informatici o telematici, nonché a dati, documenti e comunicazioni scritte.

Gli utenti sono obbligati a segnalare immediatamente ogni incidente, abuso o violazione della sicurezza, inviandone nota all'Amministratore di Sistema.

Gli utenti sono tenuti a partecipare alle iniziative di formazione organizzate dal Titolare e ad esaminare le policy emanate dal Titolare o suo delegato in materia di privacy e sicurezza informatica.

Le postazioni di lavoro portatili, i supporti informatici e la carta, quando non presidiati per periodi di tempo significativi, devono essere sistemati in armadi adeguatamente chiusi o in altri contenitori fisicamente protetti.

ARTICOLO 10 - UTILIZZO DI DISPOSITIVI PORTATILI

Nel caso di assegnazione di un personal computer portatile, di un tablet, di uno smartphone o di altro dispositivo elettronico portatile, in aggiunta a quanto già previsto, ci si deve attenere alle seguenti ulteriori disposizioni:

- il dispositivo deve essere utilizzato esclusivamente dalla persona autorizzata e solo ai fini strettamente connessi alle attività dell'Ente;

- il dispositivo non deve mai essere lasciato incustodito e comunque deve essere conservato di modo da minimizzare rischi di furto, distruzione o manomissione;

- periodicamente il dispositivo deve essere riconsegnato all'ICT ai fini della verifica della sussistenza di aggiornamenti e patch non ancora installate.

In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, e necessario informare tempestivamente l'ICT comunicando quali dati erano contenuti all'interno.

L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale e possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità alle istruzioni impartite dall'ICT.

ARTICOLO 11 - USERID E PASSWORD

L'Amministratore del Sistema assegna a ciascun dipendente autorizzato uno userid e una password che consente l'utilizzo della postazione di lavoro e l'accesso al sistema informatico del Parco (SInfP) e che lo identificano univocamente all'interno della rete.

La password é personale e non cedibile o trasmissibile a terzi fatta salva autorizzazione scritta da parte del Titolare o suo delegato: è fatto divieto a ciascun utente di divulgare, per fatto imputabile a lui direttamente o indirettamente, password, login e comunque chiavi di accesso riservate. Se smarrite va fatta immediatamente segnalazione e richiesta di sostituzione.

La richiesta di attribuzione di userid e password é effettuata dal Dirigente del Area/servizio presso il quale la persona autorizzata presta la propria prestazione lavorativa nelle modalità prescritte dall'ICT, in virtù di regolare contratto (es: rapporto di lavoro a tempo indeterminato o determinato, tirocinio, collaborazione a progetto, incarico professionale, stage ecc.).

Il Dirigente del settore/servizio, nel formulare la richiesta di accesso, indica:

- Nome/cognome della persona fisica;

- Data di inizio e fine della prestazione lavorativa;

- Gli archivi automatizzati cui dovrà accedere, specificando per ciascuno di esso anche il livello di accesso (sola lettura, lettura e scrittura); l'autorizzazione all'accesso ad un archivio automatizzato implica l'autorizzazione all'utilizzo dell'applicazione informatica preposta alla gestione e fruizione di tale base di dati.

Per una corretta gestione delle password, ciascun soggetto autorizzato e tenuto a:

- cambiare la password attribuita al primo accesso, prescindendo dal luogo da cui accede, avendo cura di impostare la password con una lunghezza di almeno 8 caratteri;

- mantenere la password riservata e non divulgarla a terzi;

- non trascrivere la password su fogli, agendine, post-it facilmente accessibili a terzi;

- in caso di scadenza della password, sostituire la password seguendo i modi e la tempistica indicata dall'Amministratore del sistema;

- non impostare la password sulla base di informazioni facilmente conoscibili, quali il proprio nome, il nome di familiari, la data di nascita, il proprio codice fiscale

- non includere la password in alcun processo di connessione automatica.

Nel caso in cui una password perda di segretezza (accidentale smarrimento della stessa, divulgazione a terzi per motivi di lavoro, ecc.), l'utente si attiva per la sua immediata sostituzione.

Quando, in relazione alle caratteristiche dell'elaboratore, non e possibile procedere all'autonoma sostituzione della password, l'utente comunica tale circostanza all'Amministratore del sistema che provvederà alla sostituzione della stessa.

Nel caso in cui il soggetto autorizzato cessi, per una qualunque ragione, la propria attività lavorativa presso la Riserva, il Dirigente dell'Area /Servizio di competenza ne da tempestiva comunicazione all'Amministratore del sistema affinché provveda alla disabilitazione dello userid.

Il soggetto autorizzato che accede a dati personali conservati in formato elettronico e tenuto a:

– chiudere le applicazioni in uso prima di allontanarsi dalla postazione di lavoro;

– impostare uno screen saver con password che si attivi dopo alcuni minuti di non operatività del computer.

ARTICOLO 12 - PROTEZIONE DEI DATI TRATTATI IN MODALITÀ TELEMATICA

Gli autorizzati al trattamento sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso; e fatto loro divieto di accedere direttamente o indirettamente a directory, files e servizi, compresi quelli di posta elettronica non dell'Ente, non espressamente e preventivamente autorizzati dall'Ente.

ARTICOLO 13 - USO DELL'ANTIVIRUS

Al fine di evitare danneggiamenti provocati dall'ingresso nel SIP di programmi contenenti virus, il Parco ha in dotazione un sistema antivirus centralizzato con aggiornamento automatico su base almeno giornaliera.

Le postazioni di lavoro sono automaticamente aggiornate ogniqualvolta l'utente si connette alla rete interna.

La persona autorizzata all'uso e tenuta a:

- evitare di introdurre applicazioni/software che non siano state preventivamente approvate dal Responsabile dell'ICT;

- verificare, con l'ausilio del programma antivirus in dotazione, ogni supporto magnetico contenente dati (cd-rom, DVD, key USB), prima dell'esecuzione dei file in esso contenuti, laddove questo non si attivi automaticamente;

- prestare sempre debita attenzione agli eventuali messaggi di segnalazione di virus contattando immediatamente

l'Amministratore del sistema in caso di anomalie;

- evitare di rispondere a mail che richiedono una conferma di lettura o che invitano a cancellarsi da mailing list;

- segnalare tempestivamente all'Amministratore del sistema i casi di spamming o comunque di ricevimento non richiesto di mail a sfondo commerciale, sessuale o finanziario;

- non partecipare ne contribuire a diffondere mail il cui testo contiene inviti alla spedizione del messaggio a quanti più utenti possibile (c.d catene di Sant'Antonio, bufale, ecc.).

L'accesso alla rete da parte di soggetti terzi (es. aziende, docenti corsi di formazione, ecc.) con computer portatili personali deve essere preventivamente comunicato dal Dirigente dell'area/Servizio competente al responsabile dell'ICT e da questi o suo delegato formalmente autorizzato previa valutazione dei requisiti di sicurezza.

ARTICOLO 14 - RISPETTO DELLA PROPRIETÀ INTELLETTUALE E DELLE LICENZE

Il software in uso nel SIP e ottenuto seguendo le procedure e le linee guida dell'Ente ed e registrato a nome della Riserva.

Ogni utente e tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright), e non può installare, duplicare o utilizzare i vari software al di fuori di quanto consentito dagli accordi di licenza.

ARTICOLO 15 - UTILIZZO DEL SOFTWARE DI PROPRIETÀ PERSONALE

Al fine di proteggere l'integrità del SIP, l'utente non può utilizzare software diverso da quello in uso nel SIP, comprese anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software detenuto a qualsiasi titolo.

CAPO III – POSTA ELETTRONICA

ARTICOLO 16 - USO DELLA POSTA ELETTRONICA

All'utente autorizzato e assegnato un account di posta elettronica da utilizzarsi limitatamente allo svolgimento di compiti e funzioni d'ufficio.

Il soggetto autorizzato e tenuto a:

- non utilizzare l'indirizzo di posta elettronica per la partecipazione a dibattiti, Forum o mailing-list, su Internet, per motivi estranei ai propri compiti e funzioni d'ufficio;

- non inoltrare messaggi, comunicazioni o circolari non attinenti la propria prestazione lavorativa (ad es. facendo dei reply to all a tutti gli altri impiegati per comunicare feste, ricorrenze o altro);

- non simulare l'identità di un altro utente per compiere operazioni di qualsiasi tipo;

- non effettuare ogni genere di comunicazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, salvo che tali operazioni, espressamente autorizzate dal Dirigente del Settore/Servizio non siano correlati ai propri compiti d'ufficio;

- non aprire allegati di posta elettronica di incerta provenienza (gli allegati possono contenere virus o codici nascosti tali da provocare la divulgazione di password e/o il danneggiamento di dati e risorse di proprietà della Riserva).

- non utilizzare sistemi client di posta elettronica non conformi agli standard adottati dall'Ente;

- non rivelare ad alcuno le proprie credenziali per l'accesso ai servizi di posta elettronica e/o di rete;

- non utilizzare il nome utente e la password di altri utenti

CAPO IV – INTERNET

ARTICOLO 17 - INTERNET

Gli utenti autorizzati sono tenuti ad utilizzare il collegamento ad Internet unicamente per motivi correlati ai propri compiti e funzioni d'ufficio, obbligandosi a:

- non utilizzare Internet per scaricare file del tipo MP3, AVI, MPG e/o altri tipi di files o programmi per la fruizione di contenuto audio/video non legati ad un uso d'ufficio;

- utilizzare internet esclusivamente per esigenze di carattere lavorativo. A tal fine il servizio ICT inibisce la consultazione di alcuni siti web non correlati all'attività istituzionale dell'Ente e, in particolare, ai siti potenzialmente lesivi per le infrastrutture dell'Ente;

- non utilizzare mezzi alternativi (modem o altro) al collegamento rete dell'Ente per connettersi ad Internet;

- non svolgere attività tese ad eludere i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software tesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo.

- Per quanto concerne le modalità di utilizzo della rete Internet per le quali valgono le medesime considerazioni generali espresse per la posta elettronica, l'utente autorizzato e tenuto a:

- non effettuare alcun tipo di transazione finanziaria ivi comprese le operazioni

- di remote banking, acquisti on-line e simili, salvo diversa ed esplicita

- autorizzazione del Dirigente di Settore/Servizio di riferimento;

- non partecipare, per motivi non professionali, a Forum, chat line, bacheche elettroniche, blog nonché registrarsi in guest book anche utilizzando pseudonimi (o nicknames);

- non scaricare software prelevato da siti Internet che non sia stato precedentemente autorizzato;

- non scaricare documenti informatici di natura oltraggiosa o discriminatoria per sesso (es: materiale pornografico, etc.), lingua, religione, razza, origine etnica, opinione o appartenenza sindacale o politica;

- non scaricare programmi per la condivisione e/o l'uso di file musicali o altro.

CAPO V – CONSERVAZIONE DEI DATI

ARTICOLO 18 - SALVATAGGIO DEI DATI MEMORIZZATI SU DISCHI DI RETE

I dati elaborati tramite il SIP sono salvati sui supporti di memorizzazione centrali (partizioni del server accessibili solo agli utenti la cui autorizzazione d'accesso e stata preventivamente creata

dall'Amministratore del Sistema sulla base delle autorizzazioni rilasciate dal Dirigente e/o Responsabile), la cui gestione e affidata al servizio ICT, il quale e dotato di un sistema che garantisce l'integrità e la disponibilità dei dati che sono assoggettati a backup al fine di evitare dispersioni o perdite d'informazioni.

ARTICOLO 19 - TRATTAMENTO DI DATI PERSONALI REGISTRATI SU SUPPORTI DI MEMORIZZAZIONE LOCALI

Al fine di salvaguardare la sicurezza dei dati personali è proibito l'utilizzo di supporti di memorizzazione locale per l'archiviazione di dati personali.

Qualora, previa espressa autorizzazione del Dirigente dell'Area/Servizio Responsabile del trattamento, siano utilizzati supporti di memorizzazione locale quali cd-rom, DVD, key USB, hard disk esterni per l'archiviazione di dati personali, il soggetto autorizzato deve osservare adeguate misure di sicurezza al fine di salvaguardare la riservatezza dei dati e la loro conservazione.

I supporti di memorizzazione utilizzati per la custodia di dati personali sono sottoposti alla seguenti restrizioni di sicurezza:

- non è consentito il riutilizzo di supporti di memorizzazione preposti alla custodia di dati personali sensibili o giudiziari, per scopi diversi da quelli relativi alle finalità del trattamento; tali supporti possono essere riutilizzati da altri solo se le informazioni contenute in tali supporti siano rese non intelligibili e tecnicamente non ricostruibili;

- i supporti di memoria non più utilizzati o non più utilizzabili sono smaltiti in modo corretto, e comunque non prima che le informazioni contenute siano rese non leggibili e tecnicamente non ricostruibili.

In particolare ciascun soggetto autorizzato deve:

- provvedere affinché i supporti informatici contenenti dati personali sensibili/giudiziari siano riutilizzati solo dopo aver cancellato i dati e le informazioni in essi contenuti, in modo che tali dati non siano in alcun modo recuperabili;

- contattare l'Amministratore del sistema in caso di riscontrate difficoltà nello svolgimento di tali operazioni, amministratore che provvederà al corretto smaltimento dei supporti stessi.

- In caso di utilizzo autorizzato di supporti memorizzazione locali, alla fine di ogni sessione di lavoro l'utente e comunque tenuto a salvare i files contenenti i dati sui supporti di memorizzazione centrali e ad eliminarli dai supporti di memorizzazione locali.