Regolamento Interno per l'utilizzo degli strumenti, servizi e risorse informatiche

Stazione Zoologica Anton Dohrn

(Approvato con delibera CdA n. 27 del 12/03/2020)

Indice

Art. 1 Premesse

Le tecnologie informatiche, le interconnessioni tra computer e l'aumento di informazioni trattate con strumenti elettronici aumentano i rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa vigente in materia. L'utilizzo da parte del personale e dei fruitori delle risorse informatiche e telematiche della Stazione Zoologica Anton Dohrn, in applicazione di quanto disposto dagli artt. 2104 e 2105 del codice civile, deve avvenire con diligenza, fedeltà e correttezza come riportato anche nel Regolamento del Personale della SZN. In tale contesto, nelle linee guida del Garante per la posta elettronica ed internet, nel Registro delle Deliberazioni n. 13 del 1° marzo 2007, vengono prescritte ai datori di lavoro alcune misure per conformare alle disposizioni vigenti il trattamento di dati personali per verificare il corretto utilizzo, nello svolgimento del rapporto di lavoro, della posta elettronica e della rete internet. L'Ufficio per lo Sviluppo e la Gestione dei Servizi Informatici & Statistici (di seguito indicato come Ufficio dei Sistemi Informativi o SIST) della Stazione Zoologica Anton Dohrn (nella figura del Responsabile SIST) cura i rapporti dell'amministrazione di appartenenza con l'Autorità per l'informatica nella pubblica amministrazione (cfr Art. 10 del D.Lgs. n.39 del 12/12/1993).

Il presente Regolamento è adottato per il corretto utilizzo nel rapporto di lavoro dei personal computer (fissi e portatili), dei dispositivi elettronici dell'Ente in generale, della posta elettronica e di internet, definendone le modalità di utilizzo nell'ambito dell'attività lavorativa e dando la massima diffusione alla cultura sulla sicurezza informatica. Le disposizioni e le prescrizioni qui indicate vanno affiancate e integrano quelle già previste nel Documento Programmatico sulla Sicurezza (DPS). In particolare, l'utilizzo delle risorse e dei servizi informatici deve avvenire:

a. nel rispetto delle leggi e norme vigenti e in particolare delle leggi in materia di sicurezza, privacy, copyright, accesso e uso dei sistemi informatici e telematici, utilizzo di beni di proprietà pubblica;
b. nel rispetto dei diritti alla riservatezza e alla dignità come sanciti dallo Statuto dei lavoratori e dal Codice sulla privacy, al fine di garantire la massima efficienza delle risorse informatiche e del loro utilizzo;
c. nel rispetto delle norme e procedure lavorative generali definite dalla SZN;
d. nel rispetto dei diritti degli altri utenti e di terzi.

La SZN deve provvedere a garantire un servizio continuativo e assicurare la riservatezza delle informazioni e dei dati, in maniera tale da evitare che comportamenti illeciti o inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati o diminuire l'efficienza delle risorse informatiche.

La SZN riconosce il valore fondamentale dell'utilizzo di strumenti di comunicazione sia nella comunicazione interna che con l'utenza esterna, anche al fine di ridurre i tempi di risposta e di migliorare pertanto l'efficienza del proprio operato.

La terminologia utilizzata nel presente regolamento è definita ai sensi del D.Lgs. 196/03 (Codice della privacy) e del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 intitolato "misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

Art. 2 Oggetto e ambito di applicazione

Il presente Regolamento contiene le disposizioni relative alle corrette modalità di utilizzo della rete e delle risorse informatiche della SZN (i server, le workstation, i personal computer, i notebook e qualsiasi altra tipologia di elaboratore elettronico, le stampanti, i plotter, le fotocopiatrici e i fax, tutti gli strumenti informatici interconnessi con la rete della SZN, gli apparati di rete, tutto il software e i dati acquisiti o prodotti da parte degli utenti o di terzi autorizzati, file di qualsiasi natura, archivi di dati anche non strutturati e applicazioni informatiche), in conformità e nel rispetto di quanto previsto dalla specifica normativa come indicato nell'Art.1 del presente Regolamento e dalle ulteriori disposizioni emanate dalla SZN.

Il presente Regolamento si applica a tutti gli Utenti: personale dipendente della SZN, senza distinzione di ruolo e/o livello, nonché tutti i collaboratori a prescindere dal rapporto contrattuale con la stessa intrattenuto (associati, assegnisti collaboratori a progetto, stagisti e borsisti, liberi professionisti, collaboratori terzi, tesisti, volontari frequentatori, visitatori, ecc.).

Art. 3 Linee guida generali

La Stazione Zoologica Anton Dohrn, consapevole delle potenzialità fornite dagli strumenti informatici e telematici, li mette a disposizione dell'Utente esclusivamente per finalità di lavoro. Non è quindi permesso utilizzare questi strumenti per altre finalità non strettamente connesse all'attività lavorativa e comunque tali da violare le normative vigenti in materia.

Nello specifico non è consentito:

a) accedere a siti e acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
b) diffondere prodotti informativi lesivi dell'onorabilità, individuale e collettiva;
c) diffondere prodotti informativi di natura politica;
d) diffondere in rete o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura;
e) svolgere ogni tipo di attività commerciale;
f) compiere attività che possano rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, supporti audio e video, clonazione o programmazione di *smart card*;
g) compiere attività che compromettano in qualsiasi modo la sicurezza delle risorse informatiche e della rete istituzionale;
h) accedere a siti di scommesse e giochi online;
i) accedere a piattaforma social, se non preventivamente autorizzati dall'Ente.

La SZN adotterà ogni accorgimento necessario a tutelarsi da eventuali comportamenti non permessi, salvaguardando il rispetto della privacy dei lavoratori. Eventuali trattamenti saranno effettuati in conformità agli obblighi di trasparenza delle Pubbliche Amministrazioni.

Art. 4 La sicurezza dei dati personali nel Regolamento UE 2019/881 (RGPD)

Allo scopo di garantire un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione Europea, il Regolamento UE 2018/1725 (RGPD) ha stabilito gli obiettivi, i compiti e gli aspetti organizzativi relativi all'ENISA (Agenzia dell'Unione europea per la Cibersicurezza). Il regolamento definisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti, processi e servizi delle Tecnologie dell'Informazione e della Comunicazione (TIC) nell'Unione, oltre che al fine di evitare la frammentazione per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione. Nel regolamento vengono definiti i compiti da parte dell'ENISA in riferimento al trattamento dei dati personali in conformità del regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio. Di seguito, gli aggiornamenti del Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione Europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (https://eur-lex.europa.eu/eli/reg/2019/881/oj).

4.1 La Direttiva (UE) 2016/1148

La direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi nell'Unione Europea (di seguito indicata come "la direttiva NIS" o NIS) adottata il 6 luglio 2016 è la prima legislazione dell'UE ad affrontare le sfide in materia di cibersicurezza, che ha permesso una prima fattiva cooperazione in termini di cibersicurezza in Europa. La NIS ha tre obiettivi principali: 1) migliorare le capacità nazionali di cibersicurezza; 2) rafforzare la cooperazione a livello dell'UE; 3) promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e i fornitori di servizi digitali.

La novità della direttiva NIS e l'urgenza di far fronte al panorama in rapida evoluzione delle ciberminacce richiedono di porre particolare attenzione nel garantire il recepimento tempestivo e efficace della direttiva. Con il termine di recepimento del 9 maggio 2018 e successivamente del termine per l'identificazione degli operatori di servizi essenziali del 9 novembre 2018, la Commissione al Parlamento Europeo sostiene da

tempo il processo di recepimento da parte degli Stati membri ed il lavoro da questi svolto nell'ottica di collaborazione e cooperazione.

4.2 Il Piano Triennale per l'Informatica.

Il Piano Triennale per l'informatica nella Pubblica Amministrazione riunisce tutti i possibili attori della trasformazione digitale del Paese (Pubblica Amministrazione, cittadini, imprese, mercato, mondo della ricerca) definendo indirizzi comuni per una strategia condivisa. Il Piano 2019-2021[1] prosegue integrando le linee di azione della versione 2017-2019 aggiornando la strategia di trasformazione digitale per lo sviluppo dell'informatica pubblica italiana con le seguenti novità:

- il recepimento delle ultime modifiche introdotte del Codice dell'Amministrazione Digitale (CAD) e delle recenti direttive e regolamenti europei sull'innovazione digitale;
- il rafforzamento del paradigma Cloud della PA con l'applicazione del principio cloud first;
- la definizione di Modelli e strumenti per l'innovazione per la PA con un'attenzione ai temi dell'*open innovation*, dell'*innovation procurement* e al paradigma *smart landscape*.

Art. 5 Titolarità, acquisizione e responsabilità individuale

La Stazione Zoologica Anton Dohrn, nella figura del suo rappresentante legale, è titolare di tutte le risorse hardware e software messe a disposizione degli utenti della SZN. Tutte le risorse informatiche assegnate devono essere custodite con cura evitando ogni possibile forma di danneggiamento. Gli Utenti sono responsabili del corretto utilizzo degli strumenti messi loro a disposizione e della loro custodia e sono tenuti a segnalare tempestivamente al SIST, eventuali guasti o difetti di funzionamento dei dispositivi hardware e software. In caso di problematiche, cattivo utilizzo e non rispetto del presente regolamento, ed incidenti che esulino da un semplice guasto tecnico, il responsabile del SIST è obbligato a dare tempestiva segnalazione al rappresentante legale della Stazione Zoologica.

Art. 6 Competenze e Responsabilità

6.1 Compiti del Responsabile dell'Ufficio dei Sistemi Informativi:

a) implementare, con l'ausilio del personale del SIST e/o di personale incaricato interno/esterno, il controllo sulla sicurezza del sistema informativo della SZN;
b) monitorare, con l'ausilio di personale incaricato del SIST, e/o di personale incaricato interno/esterno, i sistemi per individuare un eventuale uso scorretto degli stessi, nel rispetto della privacy degli utenti;
c) segnalare prontamente alla governance dell'Ente ogni attività non autorizzata sul sistema informativo della SZN;
d) attenersi scrupolosamente alle prescrizioni previste nel "Documento di adozione delle misure e accorgimenti prescritti dal Garante per la Protezione dei Dati Personali ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
e) supporto informatico e gestione delle attività istituzionali di comunicazione ed informazione della sala conferenza e delle sale multimediali, per l'organizzazione di seminari, convegni e concorsi.

Ai fini del presente regolamento, il responsabile del SIST nel ruolo di Responsabile della Transizione al Digitale (Delibera 16 del 16/11/2018) ha inoltre i seguenti compiti:

a) supporto al Direttore Generale per la predisposizione del piano triennale della transizione al digitale della SZN;
b) sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

[1](https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pubblica_amministrazione_2019_-_2021_allegati20190327.pdf)

c) sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
d) monitoraggio, attuazione e vigilanza della sicurezza informatica relativamente all'integrità dei dati (backup, antivirus, etc.), ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1 del suddetto CAD;
e) provvedere l'accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
f) report periodico sull'utilizzo delle tecnologie dell'informazione e della comunicazione;
g) monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
h) pianificazione e coordinamento della diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione.
i) pianificazione degli acquisti di beni, soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e alle esigenze di sostenibilità tecnica e sicurezza informatica;
j) predisposizione ed aggiornamento, in coordinamento con la Direzione Generale, dell'inventario dei beni informatici.

6.2 Compiti dei Responsabili delle Strutture della SZN:

a) informare il personale dipendente e/o assimilato sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo della SZN;
b) assicurare che il personale a loro assegnato si uniformi alle regole e alle procedure descritte nel presente regolamento;
c) assicurare che i collaboratori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nel presente regolamento;
d) adempiere a tutti gli obblighi inerenti alla responsabilità loro affidata in materia di trattamento di dati personali e sensibili gestiti dalla SZN;
e) segnalare prontamente al Responsabile del SIST per opportune verifiche ogni eventuale attività non autorizzata sul sistema informativo della SZN.

6.3 Compiti del personale del SIST:

a) garantire la massima riservatezza sulle informazioni acquisite direttamente o indirettamente nell'esercizio delle proprie funzioni;
b) segnalare prontamente al Responsabile del SIST ogni eventuale attività non autorizzata sul sistema informativo della SZN.

6.4 Responsabilità degli Utenti del sistema informativo della SZN:

a) il rispetto delle regole della SZN e della normativa vigente per l'uso consentito del sistema informativo;
b) l'uso delle credenziali di autenticazione loro assegnate secondo le modalità previste nel presente Regolamento;
c) la pronta segnalazione al competente Responsabile di Struttura in merito a ogni eventuale attività non autorizzata sul sistema informativo della SZN di cui vengano a conoscenza.

Art. 7 Gli strumenti Informatici

Gli strumenti informatici oggetto del presente Regolamento sono tutti i servizi e gli apparati di proprietà della SZN messi a disposizione degli Utenti al fine di permettere il quotidiano svolgimento delle proprie prestazioni lavorative.

Essi sono essenzialmente individuabili nei computer, negli apparati removibili, nei sistemi di identificazione e di autenticazione informatica, Internet e negli strumenti di scambio di comunicazioni e file, nella posta elettronica e in qualsiasi altro programma e apparecchiatura informatica destinata a memorizzare o a trasmettere dati e informazioni.
È responsabilità di tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione, di applicare e rispettare puntualmente le disposizioni del presente Regolamento.

7.1 Personal computer

Il computer è uno strumento di lavoro fornito dalla SZN e rappresenta una dotazione strumentale della sede ove è ubicato. Il suo eventuale utilizzo non inerente all'attività lavorativa è vietato perché può contribuire a innescare disservizi, costi di manutenzione e soprattutto, minacce alla sicurezza dell'intera infrastruttura tecnologica della SZN. Il computer può essere affidato a uso singolo o condiviso, sulla base della richiesta effettuata dal Responsabile della Struttura e tenuto conto della prevalenza delle funzioni che devono essere espletate. Il computer viene fornito con configurazione software predefinita che non può essere per alcun motivo modificata da parte dell'utente.

a) il ruolo di "amministratore" può essere affidato al consegnatario del bene purché le credenziali di accesso siano note al SIST che avrà cura di custodirle ed aggiornale;
b) non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
c) non è consentito utilizzare strumenti software e/o hardware privi di licenza acquisita dall'Ente;
d) non è consentito copiare sul proprio computer file contenuti in supporti magnetici, ottici e dispositivi usb non aventi alcuna attinenza con la propria attività lavorativa;
e) il computer fisso deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo;
f) in caso di postazioni condivise, occorre disconnettersi dal computer qualora ci si allontani dalla propria postazione;
g) non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche (es.: programmi di condivisione quali IRC, ICQ, torrent client, software di monitoraggio della rete in genere);
h) non è consentito configurare o utilizzare servizi diversi da quelli messi a disposizione da parte dell'Ente (quali DNS, DHCP, server internet (Web, FTP,…)) salvo previa richiesta formale;
i) non è consentito intercettare pacchetti sulla rete (sniffer) o software 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;
j) non è consentito impostare password nel bios;
k) non è consentito disassemblare il computer, asportare, scollegare, aggiungere, spostare o semplicemente scambiare tra un PC e un altro, qualsiasi apparecchiatura dell'Ente in dotazione all'Utente;
l) l'avvio del personal computer con sistemi operativi diversi da quello installato dal SIST incluse versioni live, deve essere preventivamente autorizzato per evitare possibili problemi al sistema.

Si rammenta che i dischi o le altre unità di memorizzazione locale (es. disco C:) non garantiscono il back up dei documenti frutto dell'attività lavorativa. Tali documenti e dati, non sono di proprietà privata e devono essere soggetti a salvataggio anche su unità di back up gestite dal personale incaricato del SIST.

7.2 Computer dedicati alla strumentazione

Il collegamento alla rete della SZN di computer dedicati alla strumentazione deve essere richiesto dal Responsabile della Struttura interessata all'Ufficio dei Sistemi Informativi dell'Ente che provvederà alla verifica della fattibilità e della compatibilità tecnica del collegamento. Gli interventi di manutenzione effettuati da Ditte esterne su computer collegati alla rete della SZN, devono essere preventivamente valutati dal personale del SIST. Al fine di evitare il rischio di alterazione dei risultati delle analisi non sono permessi utilizzi differenti allo scopo cui sono dedicate tali risorse. Eventuali installazioni di ulteriori programmi devono

essere preventivamente assoggettate a verifica di compatibilità e autorizzazione da parte del SIST. Al fine di poter permettere l'utilizzo condiviso di una singola risorsa da parte di più Utenti è consentita la creazione e l'uso di utenze generiche, la cui responsabilità e assegnazione è del Responsabile della Struttura. Le utenze generiche non possono effettuare trattamenti su dati personali. L'esecuzione dei backup dei dati residenti sui computer strumentali deve essere effettuata a cura del personale della Struttura che ha in carico l'apparecchiatura strumentale, in particolare: i) per computer in rete con salvataggio dei dati sul server: il backup viene eseguito automaticamente; ii) per computer non in rete o in rete senza salvataggio dei dati sul server: il backup viene effettuato dal personale del laboratorio; iii) per computer che non permettono alcun tipo di backup: sarà effettuata una valutazione da parte del SIST.

7.*3* Sistemi di calcolo avanzato *e codici di accesso*

I Sistemi di Calcolo avanzato della Stazione Zoologica di Napoli, comprendente l'infrastruttura di calcolo, i calcolatori ad alte prestazioni ed i loro programmi, le reti di collegamento locali e remote, le librerie di programmi ed il supporto fornito dal personale, sono dedicati unicamente al raggiungimento dei fini previsti dallo Statuto della SZN e nel rispetto delle leggi dello Stato e delle AUP GARR. Tale strumentazione non è di pubblico accesso ed uso e per essa, oltre alle regole indicate per gli altri strumenti informatici della SZN valgono regole specifiche.

I codici di accesso (login, password, chiavi e certificati) dovranno essere usati in modo compatibile con lo scopo per il quale sono stati assegnati e non potranno essere ceduti a terzi. I codici di accesso saranno forniti dal SIST al Responsabile della Struttura che ne farà richiesta e che gestirà autonomamente l'attribuzione alle diverse utenze. Il Responsabile della Struttura dovrà prendere ogni ragionevole precauzione per proteggere gli account forniti ed i dati da accessi non autorizzati e informerà il Responsabile del SIST tempestivamente di ogni tentativo di accesso non autorizzato.

L'utente registrato deve rispettare l'ambiente di lavoro degli altri, oltre che la natura confidenziale di qualsiasi dato o materiale che possa essere diventato disponibile, sia nel corso del normale lavoro che inavvertitamente.

L'utente registrato deve rispettare le disposizioni in vigore e le istruzioni del personale addetto per quanto riguarda l'uso delle risorse. Egli non utilizzerà le risorse per attività che influenzino negativamente la regolare operatività della rete o ne restringano l'utilizzabilità e le prestazioni per gli altri utenti e per attività che provochino trasferimenti non autorizzati di software, basi dati, etc..

7.4 Proprietà intellettuale

La Stazione Zoologica Anton Dohrn è la sola proprietaria dei diritti intellettuali associati ai propri dati, inclusi i sistemi di calcolo, programmi dal proprio personale e ai documenti prodotti, che non possono essere riprodotti o resi disponibili al pubblico in alcun modo da nessun utente senza il consenso formale dell'Ente. Gli utenti finali sono tenuti ad utilizzare i programmi ed il materiale di supporto in accordo con le condizioni previste dalla licenza d'uso.

7.5 Computer portatili e stampanti

L'Utente è responsabile dell'integrità del PC portatile affidatogli dal SIST e dei dati ivi contenuti. L'Utente è tenuto a custodirlo con diligenza sia durante l'utilizzo nel luogo di lavoro sia durante i suoi spostamenti. Ai PC portatili si applicano le regole di utilizzo previste per i personal computer. Nel caso di utilizzo comune con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati. I dischi dovranno essere protetti da password al fine di evitare, in caso di furto o di smarrimento, l'accesso a dati riservati e/o personali da parte di soggetti non autorizzati.

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a:

i. NON stampare documenti che non riguardano le proprie funzioni lavorative;
ii. stampare documenti e atti solo se indispensabili per lo svolgimento delle proprie funzioni lavorative al fine di contribuire al processo di dematerializzazione dei documenti (DPCM 13/11/2014);
iii. prediligere le stampanti di rete in luogo di quelle locali al fine di ridurre l'utilizzo di materiali di consumo (toner, cartucce);

iv. stampare in bianco/nero e fronte/retro al fine di ridurre i costi, laddove possibile.

Le stampanti locali devono essere spente ogni sera prima di lasciare gli uffici o in caso di loro inutilizzo. Qualora il dipendente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà aver cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

Art. 8 Credenziali di accesso

I sistemi di controllo degli accessi assolvono il compito di prevenire che persone non autorizzate possano accedere a un sistema informatico e alle relative applicazioni. Lo scopo è di cautelare la SZN e i suoi dipendenti da ogni tipo di manomissione, furto o distruzione di dati oltre che di limitare l'accesso a specifici dati da parte di personale non autorizzato. Inoltre, la cessione a terzi delle proprie credenziali di accesso agli strumenti informatici dell'Ente o ai portali online costituisce un rischio diretto per il possessore, in quanto gli/le potrebbero essere attribuiti illeciti o errori commessi dalla persona a cui ha ceduto le credenziali stesse.

8.1 Password

L'Utente dovrà custodire con diligenza le proprie credenziali e non comunicarle ad altre persone (es.: non scrivere la password su carta o post-it lasciandoli sulla scrivania o attaccati al monitor), non comunicare, né condividere con altri la propria password, durante la digitazione della propria password, assicurarsi che nessuno stia osservando la tastiera con l'intenzione di memorizzarla. La password deve essere composta da almeno otto caratteri e deve essere "robusta". Una password è considerata robusta quando è difficile ricostruirla e cioè quando risponde ad alcuni principi:

a. all'aumentare della sua lunghezza, aumenta la difficoltà a carpirla;
b. include cifre, lettere e caratteri speciali come: #£$ç@&!;
c. non contiene il proprio nome o cognome, il soprannome, la data di nascita, il nome di persone familiari, parole comuni, nomi di paesi, animali e così via;
d. non contiene parole che si trovano nei dizionari di qualsiasi lingua, anche se digitate al contrario, in quanto esistono software in grado di individuarle;
e. non sono composte da semplici sequenze di tasti, come ad esempio "asdfghjkl", o da ripetizioni del proprio nome utente (ad es. se il proprio utente è rossi; la password "rossi rossi" sarà inopportuna);
f. è composta con più parole contenenti errori ortografici o con sillabe combinate costituite da parole non correlate tra loro.

L'Utente si impegna a comunicare quanto prima al SIST l'eventuale furto o smarrimento della propria password. In particolare, in caso di furto, l'Utente si impegna a modificare tempestivamente la password utilizzando le procedure automatiche a sua disposizione. In ogni caso, resta inteso che l'Utente sarà responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento di tale password.

8.2 Servizio di accesso al wireless in mobilità – Eduroam

La Stazione Zoologica Anton Dohrn ha a propria disposizione l'utilizzo dei servizi di rete mediante l'utilizzo della tecnologia wireless con apparecchiature Acces Point connesse con la struttura preesistente e dislocate all'interno degli edifici dell'Ente. Per garantire la cifratura di tutto il traffico è stata attivata la modalità di sicurezza WPA seguendo le indicazioni della "Wi-Fi Alliance" con crittografia dati Advanced Encryption Standard (AES). Le credenziali di utente SZN sono automaticamente gestite dal server centrale (Radius Server) che in automatico permette la connessione alla rete solo dopo il superamento della verifica utente. Il servizio viene garantito sia attraverso ESSID SZN-WiFi facendo richiesta mediante apposito modulo, sia utilizzando la modalità d'accesso "Eduroam". La Stazione Zoologica Anton Dohrn ha aderito alla federazione Eduroam, che permette l'accesso alla rete informatica di tutti gli Istituti confederati, in tutto il mondo, utilizzando il segnale Wi-Fi trasmesso dagli Access Point (AP) distribuiti su tutto il territorio. Gli utenti della rete Wi-Fi della SZN possono utilizzare i servizi Eduroam con le stesse credenziali per l'accesso ai servizi della SZN (quali posta elettronica o ticketing, ticketing.sist.szn.it/). Per connettersi a Eduroam è necessario configurare preventivamente il proprio dispositivo. La configurazione è automatica per tutti i sistemi operativi (iOS, macOS, Windows, Linux, Android) scaricando e avviando l'apposito profilo di configurazione automatica

(CAT): https://cat.eduroam.org/?idp=2577 . Limitatamente agli ultimi tre sistemi operativi, in alternativa alla configurazione automatica, è possibile effettuare una configurazione manuale. L'autorizzazione all'accesso e alla navigazione ad internet, sia per il personale strutturato (Ricercatori, Tecnologi, Tecnici, Amministrativi) che per le altre tipologie di collaborazione con l'Ente è subordinata alla firma per presa visione ed accettazione del presente regolamento. L'utente, sottoscrivendo questo regolamento, solleva l'Istituto da ogni responsabilità per qualsiasi evento subito in proprio o arrecato a terzi durante o a seguito dell'utilizzo del collegamento Wi-Fi ad internet, assumendosi la responsabilità dell'uso del contenuto dei siti visitati, del materiale e dei messaggi trasmessi.

Art. 9 Privilegi di amministratore locale

Gli utenti che hanno responsabilità di Amministratore locale saranno tenuti ad adottare le seguenti misure minime per mantenere inalterati gli attuali livelli di sicurezza informatica dei sistemi interessati e della rete dell'Ente:

a) adozione e gestione di password definite, nella composizione e nella modalità di modifica, secondo le norme indicate nel presente Regolamento;
b) tenere traccia, ove possibile, delle operazioni effettuate su appositi file di log in occasione di nuove installazioni;
c) aderenza alle disposizioni riportate nel Documento Programmatico sulla Sicurezza adottato annualmente dalla SZN ai sensi del D. Lgs. 196/2003 Codice in materia di protezione dei dati personali.

In caso di particolari situazioni, opportunamente rappresentate e motivate al Responsabile del SIST, ove per esigenze tecniche vi siano computer per i quali l'utilizzo di particolari programmi richieda la disponibilità dei privilegi di amministrazione sulla singola macchina, l'Utente è tenuto a:

i) adottare regole e politiche per la configurazione di procedure e software di protezione;
ii) aggiornare le procedure e i software di protezione con cadenza almeno mensile.

Art.10 Rete

La rete di trasmissione dati della Stazione Zoologica rappresenta lo strumento di collegamento delle risorse informatiche dell'Ente alla Rete Italiana dell'Università e della Ricerca "GARR". Il servizio di rete è destinato principalmente alla Comunità che afferisce al GARR composta da gli Enti soci del *Consortium* GARR (CNR, ENEA, INFN e la Fondazione CRUI in rappresentanza delle Università italiane), gli organismi di ricerca vigilati dal MIUR, tra cui SZN, ASI, INAF, INGV e i Consorzi Interuniversitari per il Supercalcolo: (Almalaurea, Caspur, Cilea e Cineca accorpati in un unico consorzio). L'utilizzo rete GARR è comunque soggetto al rispetto delle *Acceptable Use Policy* (AUP) da parte di tutti gli utenti GARR. Non è consentito collegare alle prese di rete apparecchiature non previamente autorizzate quali (hub, switch, access point o altre componenti attivi e/o passivi) da parte dell'Ente. Non è inoltre consentito installare o utilizzare qualsiasi altra apparecchiatura (e.g., modem, router, Internet key) atta a gestire comunicazioni, salvo specifica autorizzazione rilasciata dall'Ente. Non è inoltre consentito effettuare spostamenti o modifiche di risorse collegate alla rete SZN (es.: pc, stampanti, fotocopiatori e altro) senza una preventiva autorizzazione da parte dell'Ente.

10.1 Risorse di rete

Gli spazi delle unità di rete messi a disposizione, sono aree di condivisione e di archiviazione di informazioni strettamente lavorative e non possono pertanto essere utilizzate per la memorizzazione di file non attinenti ad esse. In queste aree dovranno essere necessariamente salvati tutti i documenti lavorativi afferenti alla Struttura di appartenenza, al fine di renderli disponibili, in caso di necessità, agli altri utenti/colleghi della SZN. Su queste unità vengono svolte regolari attività di controllo statistico, amministrazione, backup e restore da parte del personale del SIST. Gli accessi nelle unità di rete condivise devono essere autorizzati da parte del Responsabile di sistema. Il SIST provvederà alla creazione/rimozione dei diritti di accesso e a effettuare periodicamente la verifica delle abilitazioni attive.

Possono essere fornite dall'Ente ulteriori aree deputate allo scambio di file tra strutture diverse (es.: cartella "common", file scannerizzati da scanner di rete). Onde evitare la saturazione di questi spazi, cessato lo scopo contingente, i file salvati nelle aree comuni dovranno essere rimossi a cura dell'utente che li ha memorizzati

entro un termine prestabilito e comunicato, decorso il quale verranno rimossi mediante la programmazione di apposite procedure di cancellazione automatica la cui frequenza verrà resa nota agli Utenti interessati.
Il SIST nel limite delle risorse disponibili dell'Ente, fornisce ad ogni utente una cartella ad accesso nominativo (home directory) al fine di poter archiviare documenti concernenti la propria vita lavorativa (ad esempio documenti, manuali, appunti) e per le quali non è dovuta la condivisione del contenuto con altri Utenti.
Le *home directory* hanno validità per tutta la durata della permanenza in servizio dello stesso dipendente titolare; hanno una dimensione predefinita e non estendibile. In nessuna risorsa di rete è consentito salvare file audio, video, eseguibili e archivi di posta a eccezione di quelli strettamente attinenti a esigenze lavorative e dietro specifica e motivata richiesta da parte del Responsabile di Struttura. Per tali tipologie di file e archivi sono effettuati interventi di pulizia attivati d'ufficio da parte dell'Amministratore di sistema. L'accesso straordinario alla *home directory* nominativa da parte di un soggetto terzo, può avvenire esclusivamente previa autorizzazione da parte della Direzione Generale e nei casi di prolungata assenza dal servizio o impedimento da parte del titolare della cartella che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

10.2 Internet

L'utilizzo della connessione Internet della SZN è consentita per i soli scopi lavorativi e nell'ambito delle mansioni affidate ai singoli lavoratori.
L'utilizzo degli strumenti della SZN può essere richiesto e concesso per svolgere attività che non rientrano tra i compiti istituzionali per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio per adempimenti nei confronti di pubbliche amministrazioni), purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni.
Le principali regole per l'utilizzo responsabile e corretto della rete Wi-Fi della SZN è vietato:

1) l'uso di internet per scopi vietati dalla legislazione vigente;
2) inviare, ricevere o mostrare testi od immagini che possano arrecare offesa alle persone;
3) "scaricare" o utilizzare programmi e/o dati coperti da copyright e licenze d'uso;
4) l'upload o il download di software, di documenti o file di qualsiasi altra natura, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;
5) ogni forma di registrazione utilizzando riferimenti della SZN a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
6) la partecipazione a Forum non professionali, l'utilizzo di chat, di social network, di strumenti di condivisione, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (nickname) se non espressamente autorizzati dal proprio Responsabile.
7) visitare siti che per contenuto ed immagini siano in contrasto con le finalità, l'etica e le norme della SZN;
8) utilizzare impropriamente programmi di messaggistica Istantanea e di file sharing;
9) accedere a siti VM18 o a pagamento o che offrono servizi.

Al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, o per esigenze tecniche, la SZN si avvale di appositi filtri opportunamente configurati che impediscono l'accesso a siti non ritenuti idonei e che ne comunicano la motivazione dell'impedimento. I filtri sopracitati limitano l'accesso ai siti Internet che presentano i seguenti contenuti: illegali o non etici, stupefacenti, razzismo e odio, estremismo, violenza, occultismo, plagio; materiale per adulti, nudità, pornografia; giochi, scommesse, intermediazione e trading, download di software freeware non autorizzato; social network, radio e tv via Internet (salvo i casi espressamente autorizzati dalla Direzione Generale); peer to peer; malware, spyware, hacking, bypass proxy, phishing. Qualsiasi altra tipologia di contenuti o siti che l'Ente riterrà di non dover rendere accessibile dalla rete della SZN, verrà comunicata agli utenti. La navigazione, ovvero l'accesso ai siti Internet, potrebbe avvenire previa autenticazione dell'Utente sul proxy. I file contenenti le registrazioni della navigazione sul web sono conservati, per esigenze di sicurezza, per il tempo pre-determinato secondo le norme vigenti.

10.3 Posta Elettronica

Il servizio di posta elettronica è un mezzo istituzionale di comunicazione della Stazione Zoologica e il suo utilizzo deve avvenire nel rispetto delle norme in materia di protezione dei dati personali. Sono attribuiti indirizzi di posta elettronica:

i) a Strutture Organizzative, di Funzionamento e di Ricerca e per lo svolgimento di particolari funzioni (es: direzione@szn.it, contab.amm@szn.it, assistenza-sist@szn.it);
ii) a indirizzi nominativi (es: nome.cognome@szn.it) assegnati individualmente agli utenti della SZN.

L'uso degli indirizzi di Struttura deve essere dedicato alle comunicazioni ufficiali sia interne che esterne alla SZN. Non è consentito l'utilizzo dell'indirizzo di posta nominativo o di Struttura per scopi diversi da quelli prettamente lavorativi. L'assegnazione di un indirizzo di posta elettronica avviene contestualmente all'assegnazione delle credenziali di autenticazione dell'Utente; di norma l'indirizzo di posta viene creato utilizzando "nome.cognome" e presenta il dominio istituzionale: @szn.it. I casi di omonimia sono gestiti distintamente. Oltre all'indirizzo principale è previsto l'alias "iniziale del nome.cognome@szn.it". L'accesso al servizio di posta elettronica da parte di un Utente avviene mediante delle credenziali di autenticazione (nome utente e password). Le credenziali di accesso vengono fornite direttamente all'Utente a seguito della consegna di un documento riservato contenente i dati sensibili. Tale documento può essere automaticamente inoltrato dal sistema ad un account email alternativo se fornito dall'Utente stesso al momento della richiesta. Gli utenti assegnatari delle caselle di posta elettronica sono i diretti responsabili del corretto utilizzo delle stesse e rispondono personalmente dei contenuti trasmessi. In particolare, l'Utente è tenuto a rispettare quanto segue:

a) non utilizzare il servizio per scopi illeciti o illegali o non conformi al presente Regolamento o in maniera tale da recar danno o pregiudizio alla SZN o a terzi;
b) non utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con la fruibilità del servizio da parte degli altri utenti;
c) non utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino ad esempio a: pubblicità non istituzionale, sia manifesta sia occulta; prodotti di natura politica; comunicazioni commerciali private; materiale pornografico o simile; materiale discriminante o lesivo in relazione a razza, sesso, religione; materiale che violi la legge sulla privacy; contenuti o materiali che violino i diritti di proprietà di terzi; altri contenuti illegali.

In nessun caso l'Utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili. Di seguito si elencano alcune norme di comportamento che ciascun Utente è tenuto ad osservare al fine di preservare l'efficienza del servizio di posta elettronica e delle comunicazioni con esso veicolate:

a) l'Utente è tenuto a visionare regolarmente la casella di posta elettronica di propria competenza;
b) i messaggi devono essere preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini;
c) è buona norma inviare messaggi sintetici che descrivano in modo chiaro il contenuto;
d) è necessario indicare sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parola chiave;
e) non superare la dimensione complessiva di 6 Megabyte degli allegati inviati con un singolo messaggio;
f) limitare l'invio di messaggi di posta elettronica a indirizzi plurimi (decine di destinatari) e trasmetterli solo in casi motivati da esigenze di servizio.

L'Utente, infine, si impegna a non inviare messaggi di natura ripetitiva (*catene di S.Antonio*) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

Allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali, è previsto l'uso delle liste di distribuzione (mailing list). Le caselle di posta hanno una dimensione predefinita e non estendibile, occorre pertanto mantenere in ordine la propria casella di posta provvedendo a ripulirla con regolarità e salvando gli allegati ingombranti. Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'Ente sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente,

inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare un altro dipendente a sua scelta (fiduciario) il compito di verificare il contenuto di messaggi e inoltrare al Responsabile della Struttura in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile. In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'Ente sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata e in uscita, e il dipendente non abbia delegato un altro dipendente (fiduciario), secondo quanto sopra specificato, il Responsabile della struttura cui afferisce il dipendente può chiedere all'Amministratore di sistema di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il Responsabile della Struttura deve informare il dipendente appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale. Le caselle di posta individuali hanno validità pari alla durata della permanenza in servizio del dipendente, fatte salve eventuali situazioni di congedo, distacco e comando. Nel caso in cui il dipendente non presti più la sua attività lavorativa presso la Stazione Zoologica, la casella di posta elettronica sarà prontamente disattivata. Su richiesta dell'interessato la casella di posta potrà restare attiva per ulteriori 3 mesi dalla data di cessazione del rapporto di lavoro, durante il quale sarà inserita una risposta automatica d'ufficio. Se, per esigenze lavorative, sorgesse la necessità di accedere al contenuto di tale casella di posta, il Responsabile della Struttura a cui il dipendente è assegnato potrà inoltrare motivata richiesta al Responsabile del SIST.

Art. 11 Creazione di programmi o documenti automatizzati

In caso di creazione di software e altre procedure informatiche da parte di Strutture della SZN o commissionati a soggetti terzi, devono essere resi disponibili alla SZN: a) l'accesso al codice sorgente e alle base dati; b) l'analisi e la documentazione sul funzionamento e l'installazione; c) i metadati sulle strutture dati, eventualmente implementate.
La proprietà di quanto sopra, inclusi i diritti derivanti, sono della SZN salvo il diritto di essere riconosciuto autore dell'invenzione (D.lgs. 518 del 29 dicembre 1992 che novella la legge 633/41).

Art. 12 Proprietà intellettuale e delle licenze d'uso

Tutto il software in uso nel sistema informativo della SZN in cui sia prevista una licenza d'uso deve essere registrato a nome di Stazione Zoologica Anton Dohrn. Non è possibile installare, duplicare o utilizzare software acquisiti al di fuori di quanto consentito dagli accordi di licenza. Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale, sia per quanto riguarda il software che per quanto riguarda i file di qualsiasi altra natura.

Art. 13 Crittografia e controllo dei dati informatici

Fatto salvo quanto previsto dal D.Lgs. 196/03 e successive modificazioni in materia di archiviazione, gestione, trattamento e trasmissione di dati sensibili, è fatto divieto di applicare sistemi di crittografia dati, se non espressamente richiesto e/o autorizzato dal Direttore Generale dell'Ente.

Art. 14 Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti di memorizzazione rimovibili (dischetti, hard disk esterni, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how della SZN, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, recuperato successivamente alla cancellazione. In ogni caso, i supporti contenenti dati sensibili devono essere adeguatamente custoditi in cassetti e armadi provvisti di chiusura. A tal proposito si ricorda che l'utente è responsabile non solo della custodia dei supporti ma anche dei dati dell'Ente in essi contenuti. Nel caso di utilizzo condiviso dei medesimi supporti da parte di più utenti, occorre provvedere alla cancellazione delle informazioni ivi contenute mediante programmi di formattazione a basso livello. Nel caso di smaltimento, i supporti dovranno essere precedentemente distrutti mediante punzonatura o deformazione meccanica o distruzione fisica o demagnetizzazione.

Art. 15 Protezione antivirus e firewall

Il sistema informatico e i pc collegati alla rete della Stazione Zoologica sono protetti da software antivirus aggiornati quotidianamente e da un sistema di *firewalling*. Ogni Utente è comunque tenuto a comportarsi in modo tale da ridurre il rischio di attacco al sistema informatico della SZN da parte di virus o attraverso qualsiasi altro software "aggressivo". Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste. Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente a sospendere ogni elaborazione in corso senza spegnere il computer e a segnalare l'accaduto al Responsabile del Servizio Sistemi Informativi. Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.
Ogni dispositivo magnetico di provenienza esterna alla SZN dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato all'Amministratore di sistema. Medesime condizioni dovranno essere rispettate da parte di Soggetti terzi fornitori/gestori di apparecchiature e servizi informatici che vengono utilizzati a qualsiasi titolo all'interno della rete della SZN.

Art. 16 Fax

Non è consentito installare apparati fax tradizionali o software di gestione fax diversi da quelli forniti dal SIST e previa autorizzazione e supporto da parte di quest'ultimo. Si raccomanda di non lasciare documenti incustoditi negli apparati tradizionali e nelle stampanti dedicate.

Art. 17 Teleassistenza

Per lo svolgimento di normali attività di manutenzione su personal computer connessi alla rete, il personale del SIST potrà utilizzare specifici software di connessione remota. Tali programmi vengono utilizzati per assistere l'utente al fine di effettuare interventi di assistenza informatica e di manutenzione su applicativi e hardware in uso presso l'Utente. L'attività di assistenza e manutenzione avviene previa autorizzazione da parte dell'utente interessato e possibilmente mediante visualizzazione di un indicatore visivo sul monitor dell'utente che segnala la connessione in remoto del tecnico. Le attività lavorative effettuate in condizioni di telelavoro o in smart working sono soggette alle stesse condizioni, vincoli e disposizioni del presente regolamento.

Art. 18 Monitoraggio e controlli

La Stazione Zoologica Anton Dohrn adotterà ogni accorgimento tecnico necessario a tutelare l'Ente da eventuali comportamenti non consentiti, salvaguardando il rispetto della libertà e della dignità dei lavoratori; gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza e rispetteranno il principio di pertinenza e non eccedenza.

18.1 Monitoraggio

L'Ente può effettuare, nel pieno rispetto della privacy, monitoraggi periodici su dati anonimi allo scopo di verificare l'attuazione del presente Regolamento, i possibili rischi alla sicurezza informatica e le possibili problematiche inerenti l'utilizzo degli strumenti informatici. Questi monitoraggi si possono classificare in: a) analisi del traffico di rete: effettuati attraverso specifici log dei dispositivi di rete; b) analisi del traffico Internet: effettuati attraverso specifici log dei dispositivi di connessione ad Internet; c) Inventario Hardware e Software effettuati attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete e in maniera semiautomatica per le macchine non appartenenti al dominio. Il monitoraggio delle risorse hardware e software non coinvolge in alcun modo i dati personali e i documenti presenti sulle singole postazioni di lavoro e viene effettuato per finalità organizzative e gestionali.
I dati del traffico telematico verranno gestiti secondo le modalità e le tempistiche previste dalla normativa vigente in materia di sicurezza dei dati del traffico telefonico e telematico. La Stazione Zoologica ha la facoltà di procedere di rimuovere ogni file o applicazione che riterrà pericolosa per la sicurezza del sistema informatico ovvero acquisita o installata in violazione del presente Regolamento.

18.2 Controlli

L'Ente effettua controlli periodici per verificare il rispetto del Regolamento. Il presente Regolamento costituisce, a tale proposito, preventiva e completa informazione nei confronti dei dipendenti sulla base del principio di correttezza e trasparenza (Piano Triennale di Prevenzione della Corruzione e della Trasparenza – SZN). I dati devono essere gestiti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento. Nel caso in cui emerga un evento dannoso, una situazione di pericolo o utilizzi non aderenti al presente Regolamento, che non siano stati impediti con preventivi accorgimenti tecnici o rilevati durante i monitoraggi o da attività di gestione degli strumenti informatici, l'Ente potrà adottare le eventuali misure che consentano la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati riferiti all'intera Struttura organizzativa o a sue articolazioni. Il controllo su dati anonimi si concluderà con una comunicazione al Responsabile della Struttura analizzata che si preoccuperà di inviare un avviso generalizzato relativo a un utilizzo non corretto degli strumenti della SZN, invitando i destinatari ad attenersi scrupolosamente al presente Regolamento. Qualora le anomalie e irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente alla Struttura in cui è stata rilevata l'anomalia. In caso di reiterate anomalie o irregolarità, potranno essere effettuati controlli su base individuale. L'Ente si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine esclusivo di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale. Oltre a tali controlli di carattere generale, la SZN si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno all'Amministrazione, che ledono diritti di terzi o che, comunque, sono illegittime.

Art. 19 Sanzioni

È fatto obbligo a tutti gli Utenti di osservare le disposizioni contenute nel presente Regolamento. Il mancato rispetto o la violazione delle indicazioni ivi contenute è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dai vigenti CCNL, nonché con le azioni civili e penali conseguenti previste dalla normativa vigente in materia. Ogni dipendente dovrà assumersi la piena responsabilità per le proprie azioni e dovrà farsi garante per la Stazione Zoologica Anton Dohrn e tenerla indenne da responsabilità e richieste di rimborsi di danni, avanzate da soggetti terzi. Con riferimento ai collaboratori e/o prestatori d'opera, qualora questi per l'espletamento del loro incarico si servissero degli strumenti della SZN, deve essere previsto l'obbligo di rispettare il presente Regolamento, con diritto della SZN, nei casi di violazione, di risolvere il contratto stesso.

Art. 20 Entrata in vigore

Il presente Regolamento entra in vigore alla data della sua approvazione e pubblicazione sul sitoweb istituzionale della SZN. Il presente Regolamento è soggetto a revisione periodica e sulla base degli aggiornamenti normativi e tecnologici nonché sulla base delle nuove esigenze di sicurezza.