ISTITUTO ZOOPROFILATTICO SPERIMENTALE DEL LAZIO E DELLA TOSCANA M. ALEANDRI

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO

Num. 156/24 Del. 17/04/2024

Oggetto:

"Presa d'atto e adozione del Regolamento per l'utilizzo delle risorse infrastrutturali e del patrimonio informatico dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri"

Proposta di deliberazione n.	163/24
Data Proposta di deliberazione	15/04/2024
Struttura	AMM_STS UNITÀ OPERATIVA TECNICO-PATRIMONIALE E INGEGNERIA CLINICA
L'Estensore	BURATTI CLAUDIA
Il Responsabile del procedimento	PACE ERMINIO
Responsabile della Struttura	PACE ERMINIO

Visto di Regolarità contabile	
N. di prenotazione	

IL Direttore Amministrativo
Dott. Manuel Festuccia

IL Direttore Sanitario
Dr. Giovanni Brajon

IL Commissario Straordinario
Dr. Stefano Palomba

%firma%-1 %firma%-3

Firmato digit. dal Resp. Struttura: PACE ERMINIO
Firmato digit. dal Dir. Amministrativo: FESTUCCIA MANUEL
Firmato digit. dal Dir. Sanitario: BRAJON GIOVANNI
Firmato digit. dal Commissario Straordinario: PALOMBA STEFANO

Il Dirigente proponente, con la sottoscrizione del presente atto, a seguito dell'istruttoria effettuata attesta, ai fini dell'art. 1 della L. 20 del 1994, così come modificato dall'art. 3 della L.639 del 1996, che l'atto è legittimo nella forma e nella sostanza ed è utile per il servizio pubblico.

(Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa)

IL RESPONSABILE DELLA UOC TECNICO PATRIMONIALE, INGEGNERIA CLINICA E SISTEMI INFORMATICI
Ing. Erminio Pace

OGGETTO: "Presa d'atto e adozione del Regolamento per l'utilizzo delle risorse infrastrutturali e del patrimonio informatico dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri"

PREMESSO che

- è necessario uniformarsi alla vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679, alla legge n. 300/1970 (Statuto dei lavoratori) e ai provvedimenti emanati dall'Autorità Garante (in particolare il Provvedimento del 1 marzo 2007);

- è opportuno regolamentare l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica, di proprietà dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri, al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli o scorrette che potrebbero esporre l'ente a problematiche di sicurezza, di immagine e patrimoniali;

- è opportuno rendere edotta l'utenza circa le responsabilità e i limiti di utilizzo assunte a seguito dell'assegnazione di beni aziendali;

CONSIDERATO che

- è opportuno uniformarsi ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, in conformità al Codice di comportamento adottato (Allegato C - delibera n°40 del 31/01/2014);

RITENUTO

- di dover procedere all'adozione di un nuovo Regolamento Informatico che fornisca le metodiche per un corretto utilizzo delle risorse infrastrutturali e del patrimonio informatico dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri;
-di dover definire l'ambito di applicazione, le modalità e le norme da adottare nell'utilizzo della strumentazione informatica di proprietà dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri;

DATO ATTO che

-l'utilizzo accorto e oculato delle risorse informatiche garantisce la minimizzazione dei rischi inerenti la sicurezza informatica e, quindi, la conseguente riduzione della probabilità di interruzioni nei servizi dovuti ad hackeraggi e/o a perdita di immagine per dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri
- l'utilizzo di metodiche e procedure standardizzate garantisce l'efficentamento dei servizi all'utenza e una maggiore tempestività nella risoluzione delle criticità di natura informatica, divenute cruciali e indispensabili nelle attività operative dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri;

VISTO

- il D.lgs. 31 marzo 2023, n. 36 “Codice dei contratti pubblici in attuazione dell’articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici”;
- il Regolamento (UE) 2016/679;
- la legge n. 300/1970 “Statuto dei lavoratori”;

PROPONE

1. di adottare il Regolamento per l’utilizzo delle risorse infrastrutturali e del patrimonio informatico dell’Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri (All. n° 1) e il suo allegato (All. n° 2).

Direttore UOC Tecnico Patrimoniale
Ingegneria Clinica e Sistemi Informatici
Il Dirigente Erminio Pace

IL COMMISSARIO STRAORDINARIO

Oggetto: "Presa d'atto e adozione del Regolamento per l'utilizzo delle risorse infrastrutturali e del patrimonio informatico dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri"

VISTA la proposta di deliberazione avanzata dal Direttore della U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici avente ad oggetto: "Presa d'atto e adozione del Regolamento per l'utilizzo delle risorse infrastrutturali e del patrimonio informatico dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri"

PRESO ATTO che il Direttore proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è legittimo e utile per il servizio pubblico;

SENTITI il Direttore Amministrativo e il Direttore Sanitario che hanno espresso parere favorevole alla adozione del presente provvedimento;

RITENUTO di doverla approvare così come proposta,

DELIBERA

Di approvare la proposta di Deliberazione avente ad oggetto: "Presa d'atto e adozione del Regolamento per l'utilizzo delle risorse infrastrutturali e del patrimonio informatico dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri", sottoscritta dal Responsabile dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici, da considerarsi parte integrante e sostanziale del presente provvedimento, rinviando al preambolo ed alle motivazioni in essa contenute e conseguentemente:

2. adotta il Regolamento per l'utilizzo delle risorse infrastrutturali e del patrimonio informatico dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri (All. n° 1) e il suo allegato (All. n° 2).

IL COMMISSARIO STRAORDINARIO
Dr. Stefano Palomba

Verbale di consegna e presa in carico di risorse informatiche

Il sottoscritto _____ dipendente/non dipendente/ricerca, dell'IZSLT afferente alla U.O. _____, con il ruolo di _____, consapevole delle responsabilità e delle conseguenze civili e penali previste in caso di dichiarazioni mendaci, dichiara di conoscere il regolamento informatico aziendale ed, in particolare, i Capi III°, IV° e V°, e di essere assegnatario solo ed esclusivamente delle risorse informatiche elencate di seguito:

Q.tà	Tipo	Marca	Modello	N.Gen	N.Seriale

Luogo e Data di consegna

Il Dipendente

Istituto Zooprofilattico Sperimentale del Lazio e della Toscana *M. Aleandri*

REGOLAMENTO INFORMATICO AZIENDALE

Utilizzo delle risorse infrastrutturali e del patrimonio informativo dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana *M. Aleandri*

SOMMARIO

CAPO I – PRINCÌPI

Art. 1 – Introduzione, Definizioni e Finalità

Il presente regolamento ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione di proprietà dell'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana *M. Aleandri*, da parte degli utenti assegnatari al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli o scorrette che potrebbero esporre l'ente a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali da adottare è ispirato ai princìpi di diligenza, informazione, correttezza nell'ambito dei rapporti di lavoro, derivanti dal Codice di comportamento (Allegato C - delibera n°40 del 31/01/2014) e inoltre finalizzato a prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano.
A tale proposito si rileva che gli eventuali controlli previsti escludono finalità di monitoraggio diretto e intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679, alla legge n. 300/1970 (Statuto dei lavoratori) e ai provvedimenti emanati dall'Autorità Garante (in particolare Provvedimento del 1° marzo 2007).

Art. 2 – Ambito di applicazione

Il presente regolamento si applica a ogni utente assegnatario di beni e risorse informatiche aziendali, ovvero utilizzatore di servizi e risorse informative dell'ente.

- Per **utente** pertanto si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, borsista, ricercatore, consulente, fornitore o altro che in modo continuativo non occasionale operi all'interno dell'organizzazione aziendale utilizzandone beni e servizi informatici.
- Per **ente** si intende, invece, la società, l'organizzazione e in generale il titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza. In questo ambito, rappresentato dall'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana *M. Aleandri,* con sede legale in Via Appia Nuova 1411, 00178, Roma.
- Per **risorse infrastrutturali** si intendono tutte le componenti hardware/software e gli apparati elettronici.
- Per **patrimonio informativo** si intende l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Art. 3 – Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT[1] e le reti informative costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà dell'ente.
Ciò considerato, il loro utilizzo è consentito solo per finalità di adempimento delle mansioni lavorative affidate a ciascun utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti all'attività svolta per l'ente, e comunque per l'esclusivo perseguimento degli obiettivi aziendali.
A tal fine si precisa sin d'ora che qualsivoglia dato o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'ente sarà dallo stesso considerato come avente natura aziendale e non riservata.

Art. 4 – Responsabilità personale dell'utente

Ogni utente è responsabile civilmente e penalmente del corretto utilizzo dei beni e delle risorse informatiche affidatigli dall'ente nonché dei relativi dati trattati per finalità aziendali.
A tal fine ogni utente, nel rispetto dei princìpi di diligenza sottesi al rapporto instaurato con l'ente e per quanto di propria competenza, è tenuto a tutelare il patrimonio aziendale da utilizzi impropri o

1 *(Information and Communication Technologies) Tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni.*

non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è e rimane sempre quello di preservare l'integrità e la riservatezza dei beni, dei dati, delle informazioni e delle risorse aziendali.
Ogni utente è tenuto a operare a tutela della sicurezza informatica aziendale, in relazione al proprio ruolo e alle mansioni in concreto svolte, riportando al proprio responsabile organizzativo diretto e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente regolamento. Sono vietati comportamenti che possano creare un qualsiasi danno, anche di immagine, all'ente e agli altri utenti.
L'assegnazione della Risorsa informatica non ne comporta il possesso, in quanto trattasi di strumento di esclusiva proprietà aziendale. L'utente utilizza, per il proprio lavoro, soltanto risorse assegnatigli dall'ente. L'uso di apparecchiature private deve essere preventivamente autorizzato dal Dirigente della U.O. di riferimento, secondo le modalità indicate nel successivo paragrafo 15.

Art. 5 – Controlli

L'ente esclude la configurabilità di forme di controllo aziendali aventi direttamente a oggetto l'attività lavorativa dell'utente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, statuto dei lavoratori).
Ciononostante, non si esclude che si possano utilizzare sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori per motivi di sicurezza e protezione dei dati. La suddetta attività può essere soggetta a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e può essere messa a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza dei dati derivati dall'attività sulla rete dell'ente da parte dell'utente è soggetta a quanto dettato dal D.lgs. n. 196/2003 e S.M.I.
È responsabilità del Dirigente di struttura verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato.
Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'ente effettua con gradualità, nel rispetto dei princìpi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

- Analisi aggregata del traffico di rete riferito all'intera struttura lavorativa o a sue aree (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo delle risorse infrastrutturali (hardware e software).
- Nel caso in cui si dovessero riscontrare violazioni del presente regolamento, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite;
- In caso di successivo permanere di una situazione non conforme o dove siano rilevate ulteriori violazioni, si potrà procedere con un'analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.
- Nonostante l'adozione delle sopra elencate misure, se i fatti possono essere sospettati di costituire un reato, l'Ente potrà valutare la trasmissione delle informazioni alla Procura della Repubblica

L'ente non utilizza sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività eseguita del lavoratore, fatta eccezione per quanto inerente alle attività in smartworking.

Capo II — MISURE ORGANIZZATIVE

Art. 6 – Amministratore di sistema

L'ente conferisce agli operatori informatici dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici le funzioni di amministratore di sistema con il compito di:

- Sovrintendere ai beni e alle risorse informatiche aziendali;
- Gestire l'hardware e il software di tutta la dotazione informatica di proprietà dell'ente;
- Gestire la creazione, l'attivazione, la disattivazione e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse (PC, Laptop, Posta elettronica, VPN ecc.), previamente assegnati agli utenti;
- Supervisionare la presenza di account utente con privilegi di amministratore non autorizzati
- Il monitoraggio del corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché rientri nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- La creazione, la modifica e la rimozione di qualunque account o privilegio purché rientri nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- La rimozione di software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché rientri nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- Provvedere alla sicurezza informatica dei sistemi informativi aziendali;
- Eliminare, senza previa comunicazione, ogni software non autorizzato, secondo le modalità indicate nel successivo paragrafo 15, o fattore che possa comportare una riduzione del livello di sicurezza informatica non appena ne vengono a conoscenza.

Art. 7 – Assegnazione degli account e gestione delle password

7.1 – Creazione e Gestione degli Account

Un account utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali per singola postazione lavorativa. Gli account utenti vengono creati dagli operatori informatici della U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici e sono personali, cioè associati univocamente alla persona assegnataria. Ogni utente è responsabile dell'utilizzo del proprio account utente.

L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione", username e password, solitamente comunicate all'utente dal personale afferente alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici che le genera con modalità tali da garantirne la segretezza.

Le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi, anche a soggetti in posizione apicale all'interno dell'ente.

Se l'utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, è tenuto a modificare immediatamente la password e a segnalare, per iscritto, la violazione al proprio Dirigente e al responsabile privacy aziendale.

In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive aziendali o per la sicurezza e operatività delle risorse informatiche, l'ente si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente.

Non sono previsti account anonimi, nel caso di creazione di profili generici (per es. nome dell'unità) in assenza di diversa indicazione la responsabilità è attribuita al Direttore dell'unità.

I beni e la strumentazione informatica oggetto del presente regolamento rimangono di esclusivo dominio dell'ente, che in conseguenza dei rapporti instaurati con gli utenti ne disciplina l'assegnazione.

7.2 – Gestione e Utilizzo delle Password

A seguito della prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'utente ha il compito di modificare al primo utilizzo la propria password procedendo allo stesso modo ogni 6 mesi.
L'utente, nel definire il valore della password, deve rispettare le seguenti regole:

- Utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, ecc.), di cui almeno uno numerico;
- La password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#$£$%...";
- Evitare di includere parti del nome, cognome o comunque elementi a lui agevolmente riconducibili;
- Evitare l'utilizzo di password comuni o prevedibili;
- Proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi;
- La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.
- Le password utilizzate hanno una durata massima di sei mesi, trascorsi i quali le password devono essere sostituite.

Scrivere la password su post-it o altri supporti non è conforme alla normativa, compromette in maniera pressoché totale le misure di sicurezza previste, costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

7.3 – Cessazione degli Account

In caso di interruzione del rapporto di lavoro con l'utente, le credenziali di autenticazione verranno disabilitate entro un periodo massimo di 30 (trenta) giorni dalla data della formale comunicazione del Direttore della UOC Risorse Umane e Affari Legali al Direttore dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici; entro 90 (novanta) giorni, invece, si disporrà la definitiva e totale cancellazione dell'account utente.
Casi particolari andranno valutati singolarmente, dopo autorizzazione formale rilasciata secondo le modalità indicate nel successivo paragrafo 15.

Art. 8 – Postazioni di lavoro

Per postazione di lavoro si intende il complesso unitario di personal computer (di seguito pc), notebook, tablet, smartphone, accessori, periferiche e ogni altro dispositivo (*device*) concesso in utilizzo all'utente. L'assegnatario di tali beni e strumenti informatici aziendali ha il compito di farne un uso compatibile con i princìpi di diligenza sanciti nel Codice civile e da questo regolamento.
Al fine di disciplinare un corretto utilizzo di tali beni l'ente ha adottato le seguenti regole tecniche:

- Ogni pc, notebook (accessori e periferiche incluse), tablet, smartphone o altro dispositivo (*device*), sia esso acquistato, noleggiato o affidato in locazione, rimane di esclusiva proprietà dell'ente ed è concesso all'utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti all'attività svolta.
- È dovere di ogni utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente.

- Il pc e gli altri dispositivi di cui sopra devono essere utilizzati solo con hardware e software autorizzati dall'ente. Per utilizzare software o applicativi non presenti nella dotazione standard fornita è necessario che il proprio Dirigente ne faccia espressa richiesta con le modalità indicate nel successivo paragrafo 15.
- Le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive.
- Quando un utente si allontana dalla propria postazione di lavoro deve bloccare la sessione di lavoro con la combinazione di tasti WINDOWS + L o effettuare il log-out della sessione (disconnetti utente).
- L'utente deve segnalare con la massima tempestività al proprio Dirigente di riferimento eventuali guasti e problematiche tecniche rilevati o il malfunzionamento delle apparecchiature, il quale inoltrerà richiesta di assistenza alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici tramite apposito sistema di ticketing[2] e secondo le modalità indicate nel successivo paragrafo 15.
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi.
- **L'ente, attraverso il personale informatico afferente alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici, si riserva la facoltà di rimuovere d'ufficio e senza alcun preavviso qualsiasi elemento hardware o software la cui installazione non sia stata eseguita dal medesimo personale afferente alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici e preventivamente autorizzata, con le modalità indicate nel successivo paragrafo 15.**

L'utente deve segnalare con la massima tempestività al proprio Dirigente eventuali guasti, problematiche tecniche, malfunzionamenti delle apparecchiature informatiche e ogni eventuale utilizzo non conforme al presente regolamento inerente alla propria postazione di lavoro e a quella di un suo collega, affinché quest'ultimo inoltri richiesta di assistenza alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici, secondo le modalità indicate nel successivo paragrafo 15.

Gli apparecchi di proprietà personale dell'utente quali computer portatili, telefoni cellulari, smartphone, agende palmari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali e qualsiasi altro dispositivo non potranno essere collegati ai computer o alle reti informatiche aziendali salvo preventiva richiesta di autorizzazione scritta, eseguita con le modalità indicate nel successivo paragrafo 15.

8.1 – Protezione da virus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus, malware o altro software aggressivo. Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer.
- scollegare il computer dalla rete tramite rimozione fisica del cavo di rete
- tentare la rimozione del virus attraverso gli strumenti forniti dall'antivirus stesso
- In ogni caso, è necessario segnalare l'accaduto al proprio Dirigente di riferimento che inoltrerà richiesta di assistenza alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici tramite apposito sistema di ticketing e secondo le modalità indicate nel successivo paragrafo 15.

2 Un sistema di ticketing è uno strumento software progettato per organizzare e distribuire le richieste di assistenza dei clienti in entrata.

E' fortemente sconsigliato l'utilizzo di CD-ROM, cd riscrivibili, dvd, pen drive, hard-disk esterni, memory card e ogni altro supporto di memorizzazione di provenienza ignota. Ogni dispositivo di memorizzazione dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, l'utente dovrà seguire le indicazioni sopra riportate e consegnare il dispositivo al personale dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici. L'utilizzo di tali dispostivi è consentito previa autorizzazione rilasciata dal Dirigente della U.O. di appartenenza, secondo la metodologia descritta al successivo paragrafo 15.

8.2 –Teleassistenza

Relativamente alle attività di manutenzione remota su personal computer connessi alla rete aziendale, il personale tecnico dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici potrà utilizzare specifici software. Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware. La configurazione del software prevede un indicatore visivo sul monitor dell'utente che segnala quando il tecnico è connesso al personal computer.

Art. 9 – Nuove assunzioni, sospensioni e cessazioni

Ogni nuova assunzione e sospensione (es. comando, aspettativa) del rapporto di lavoro dell'utente nei confronti dell'ente, deve essere oggetto di comunicazione ufficiale da parte del Direttore della U.O. di appartenenza tramite l'apposito sistema di ticketing e secondo le modalità indicate nel successivo paragrafo 15. In detta comunicazione il Direttore della U.O. di appartenenza potrà richiedere, motivandolo, l'attivazione delle seguenti funzionalità:

- Creazione/dismissione account di posta aziendale
- Creazione/dismissione account di applicativi istituzionali (es. Sito istituzionale, Cespiti, Sistema di ticketing)
- Attribuzione/disattivazione servizi specifici (es. VPN, Remote desktop)
- Aggiornamento liste di distribuzione posta (tutti i dipendenti, solo comparto, solo dirigenza)

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 10 – Utilizzo delle risorse infrastrutturali

10.1 – Utilizzo del personal computer

Il personal computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo improprio può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso al dispositivo è protetto da una password, strettamente personale, che deve essere custodita dall'utente con la massima diligenza e non divulgata. Le password devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che lo preveda e per lo screen-saver.

Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Direttore dell'U.O.C. di competenza e del Direttore dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici, conseguite con le modalità indicate nel successivo paragrafo 15. Il Direttore dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici e lo staff da lui diretto, per l'espletamento delle funzioni e mansioni assegnate e tipicamente per attività di manutenzione, ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, in relazione agli scopi di volta in volta identificati, garantendo comunque la riservatezza delle informazioni.
In nessun caso è consentito all'utente di procedere, autonomamente, all'installazione di programmi. In caso di necessità di installazione di software applicativi e/o procedure in aggiunta alla dotazione originaria, l'intervento deve essere autorizzato dal Dirigente della UO coinvolta, con le modalità indicate nel successivo paragrafo 15. Il personale informatico, afferente alla UOC Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici, provvederà con modalità atte a garantire la piena compatibilità funzionale e tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti, nonché per mantenere alto il livello di sicurezza informatica dei sistemi dell'Ente. Sussiste infatti il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni del dispositivo o del sistema operativo.
Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana M. Aleandri (DLgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).
Non è consentito, in nessun caso, all'utente effettuare modifiche alle caratteristiche impostate sui PC in dotazione, sui punti rete di accesso e alle configurazioni delle reti LAN/WAN presenti nelle sedi.
Non è consentito, in nessun caso, all'utente rimuovere, danneggiare, modificare le caratteristiche tecniche e funzionali impostate né asportare componenti hardware nel pc assegnato in uso.
Non è consentito all'utente caricare o inserire all'interno del personal computer assegnato in uso dati personali non attinenti all'attività lavorativa svolta.
Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o almeno una volta a settimana in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un dispositivo incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Per tale motivo si richiede all'utente di bloccare la postazione prima di assentarsi (combinazione di tasti WINDOWS+L).
Non è consentita l'installazione sul proprio personal computer o il collegamento sulla rete LAN di nessun dispositivo di memorizzazione, se non autorizzata espressamente del Dirigente della U.O. di afferenza, secondo le modalità indicate nel successivo paragrafo 15.
Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

In ogni caso, al fine di evitare o ridurre la possibile circolazione di dati personali sul medesimo apparecchio, gli utenti devono cancellare tutti quelli eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione. In caso contrario gli operatori della U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici possono procedere alla cancellazione, senza previa comunicazione.

Gli operatori della U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici sono tenuti, senza previa comunicazione, a cancellare software e documentazione non pertinente, inappropriata, fonte di pericolo informatico o, comunque, non installata previa specifica autorizzazione. Nei casi dubbi, gli operatori della U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici possono richiedere delucidazioni al Dirigente della U.O. nella quale opera il lavoratore assegnatario del dispositivo.

10.2 – Utilizzo della rete

L'accesso alla rete è consentito solo attraverso dispositivi abilitati, e solo attraverso account istituzionali. Eventuali accessi straordinari vanno comunicati per tempo e autorizzati, tramite l'apposito sistema di ticketing e secondo le modalità indicate nel successivo paragrafo 15.
L'accesso alla rete è consentito per sole finalità lavorative. Ogni tipo di utilizzo non autorizzato verrà considerato abuso.
Il personale afferente alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici opera al fine di garantire un'istallazione sicura e conforme.

10.3 – Utilizzo delle unità di archiviazione di rete (NAS)

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, sono svolte regolari attività di controllo e amministrazione da parte del personale dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici.
Gli accessi alle unità devono essere approvati dal Direttore dell'U.O. secondo le modalità indicate nel successivo capitolo 15. Il personale afferente alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici si occuperà di assegnare le giuste autorizzazioni, garantendo la riservatezza dei dati.
La condivisione di cartelle e/o file e in generale del contenuto delle unità deve essere approvata dal Dirigente della UO richiedente e autorizzata secondo le modalità indicate nel successivo paragrafo 15.
Il personale dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici è tenuto, senza previa comunicazione, a rimuovere ogni file o applicazione non istallata dal medesimo personale informatico, non autorizzata, ritenuta pericolosa per la sicurezza o non pertinente all'attività lavorativa svolta, rinvenuta sui personal computer degli utenti o sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti da evitare un'archiviazione ridondante.

10.4 – Modalità di accesso alla rete e ai servizi/programmi utenti esterni

Per essere autorizzati all'uso delle risorse informatiche e dei relativi servizi, è necessario che, anche nel caso di utenti esterni, il Dirigente dell'Unità Organizzativa presso cui devono prestare la propria attività lavorativa presenti richiesta scritta e motivata, tramite l'apposito sistema di ticketing e secondo le modalità indicate nel successivo paragrafo 15.
Il personale informatico afferente all'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici provvede alla creazione di un account per l'accesso alla rete con i privilegi minimi necessari per l'attività che deve essere svolta.

10.5 – Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nella UO di lavoro. Se i PC portatili sono condivisi da più persone, sarà compito del responsabile dell'UO vigilare che il PC sia usato in modo appropriato.
Ai PC portatili si applicano le regole di utilizzo previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
In relazione alle condizioni in cui si troverà a lavorare l'utente fuori sede, che siano attività a breve scadenza tipo convegni o corsi, che sia un'attività continuativa tipo smartworking o che si tratti di

viaggi all'estero, le misure di prevenzione e di sicurezza verranno valutate, di volta in volta, al fine di proteggere la privacy dell'utente e i dati presenti sui dispositivi che ha in dotazione.
In caso di furto, danneggiamento o smarrimento del PC portatile l'utente assegnatario dovrà darne immediato avviso alla Direzione Generale dell'ente; se tali eventi siano riconducibili a un comportamento negligente o imprudente dell'utente stesso o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;

10.6 – Utilizzo delle postazioni di stampa e dei materiali di consumo

L'utilizzo delle postazioni di stampa e dei materiali di consumo in genere (carta, inchiostro, toner, supporti digitali come CD-ROM e dvd) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.
Non è consentito lasciare incustoditi presso le stampanti documenti cartacei contenenti dati sensibili o riservati, al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa. L'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana *M. Aleandri* predilige l'utilizzo delle stampanti centralizzate di rete con funzione di stampa, copia e scansione in un'ottica di ottimizzazione delle risorse economiche e aggiornamento continuo della dotazione tecnologica, limitando quindi l'uso e l'acquisto di nuovi dispositivi di stampa locali.
L'utilizzo di fax per l'invio di documenti che hanno natura strettamente confidenziale è generalmente da evitare. In caso ciò sia necessario si deve preventivamente avvisare il destinatario in modo da ridurre il rischio che persone non autorizzate possano venire a conoscenza del contenuto della comunicazione e successivamente chiedere la conferma telefonica di avvenuta ricezione.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria, e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio files di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

10.7 – Software

L'installazione di software privi di regolare licenza non è consentita in nessun caso.
L'istallazione di un software aggiuntivo può essere eseguita soltanto dal personale afferente alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici. Per istallare un software il Dirigente della U.O. di competenza deve fare richiesta tramite l'apposito sistema di ticketing e secondo le modalità indicate nel successivo paragrafo
Il personale afferente alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici software è tenuto a cancellare, senza previa comunicazione, eventuali software installati in modo non conforme al presente regolamento, anche se dotati di licenza open-source.
Tutti gli utenti sono tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza.
Non è consentito eseguire il download o l'upload di software non autorizzato.
Considerato quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi soggette alle sanzioni previste dalla legge che comprendono il risarcimento del danno, il pagamento di multe e anche la reclusione.
La duplicazione illegale del software non è giustificabile e non è tollerata, costituisce violazione del presente regolamento ed espone alle sanzioni disciplinari previste.

10.8 – Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files o documenti esternamente al computer: CD-ROM, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.
L'utilizzo di tali supporti risponde alle direttive di seguito riportate:

- Non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'ente (per le modalità operative fare riferimento a quanto riportato all'art. 15 – Comunicazioni);
- È onere dell'utente custodire i supporti contenenti categorie particolari di dati (art. 9 GDPR) onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto;
- Non è consentito importare sulla stazione di lavoro aziendale, o su risorse dell'Ente, files non aventi alcuna attinenza con la propria prestazione lavorativa.
- Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati / installati / testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo da parte del personale dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici.

Qualsiasi dispositivo, una volta connesso all'infrastruttura informatica dell'ente, sarà soggetto (ove ciò sia compatibile) al presente regolamento.

10.9 – Strumenti di fonia mobile o di connettività in mobilità

A seconda del ruolo o della funzione svolta, l'ente può rendere disponibili impianti di telefonia fissa e mobile e dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in Internet tramite rete dati che del servizio di telefonia tramite rete mobile.
Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale concesso in uso per scopi esclusivamente lavorativi. È tuttavia permesso un utilizzo personale sporadico e moderato dei telefoni aziendali utilizzando la "diligenza del buon padre di famiglia" prevista dalla normativa e comunque tale da non ledere il rapporto fiduciario instaurato con il proprio datore di lavoro.
Al fine di controllo del corretto utilizzo dei servizi di fonia aziendale l'ente può esercitare i diritti di cui all'art. 124 D.lgs. 196/2003 (fatturazione dettagliata) richiedendo ai provider di telefonia i dettagli necessari agli accertamenti sull'uso e relativo costo del traffico effettuato nel tempo.
I controlli saranno eseguiti secondo criteri e modalità descritte all'art. 5 del presente regolamento. Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo l'ente potrà richiedere il tabulato analitico delle chiamate effettuate dalla SIM in carico ad un utente per tutto il periodo di interesse.
L'utilizzo dei dispositivi mobili risponde alle seguenti regole:

- Ciascun utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e conseguentemente, anche della sua diligente conservazione;
- I dispositivi devono essere dotati di password di sicurezza, per esempio codice PIN del dispositivo, che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che:
  - il codice PIN dovrà essere composto da quattro o più cifre numeriche, altri codici di accesso dovranno garantire analoga protezione;
  - il codice PIN o altri codici di accesso dovranno essere modificato dall'assegnatario con cadenza al massimo semestrale;
- ogni utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione all'ente.
- In caso di furto, danneggiamento o smarrimento del dispositivo mobile l'utente assegnatario dovrà darne immediato avviso alla Direzione Generale dell'ente; se tali eventi siano riconducibili a un comportamento negligente o imprudente dell'utente stesso o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;
- Non è consentito all'utente caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare o almeno

ridurre la circolazione di dati personali sull'apparecchio, è obbligatorio cancellare tutti i dati eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione;

- Non è consentito all'utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi a meno che non siano strettamente connesse con il proprio compito lavorativo e siano preventivamente autorizzate dall'ente;
- L'installazione di applicazioni, gratuite o a pagamento, su smartphone e tablet deve essere espressamente autorizzata, rimanendo in caso contrario a carico dell'utente le responsabilità derivanti dall'installazione non autorizzata che costituisce violazione del presente regolamento;
- Salvo diversi specifici accordi derivanti da esigenze di servizio, al momento della consegna di tablet o smartphone l'utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che in caso contrario l'ente potrebbe venire a conoscenza, seppur accidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

Capo IV — GESTIONE DELLE COMUNICAZIONI TELE-MATICHE

Art. 11 – Gestione utilizzo della rete internet e dei relativi servizi

Il personal computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa, dunque ciascun utente potrà essere abilitato alla navigazione Internet e pertanto si richiamano tutti gli utenti a una particolare attenzione al suo utilizzo consapevole così come dei servizi collegati, in quanto ogni operazione posta in essere è associata al MAC address[3] e all'indirizzo IP[4] assegnato dall'ente.

Prima di connettersi ad una rete internet diversa dell'Istituto è importante accertarsi che la stessa sia considerata sicura.

La connessione a Internet, in quanto strumento a disposizione degli utenti per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in modo da prendere ogni precauzione conseguente. Data la vasta gamma di attività aziendali, non è possibile definire a priori un elenco di siti aziendali autorizzati. Tuttavia, la Direzione Generale dell'ente potrà attivare appositi strumenti di filtraggio, mediante i quali bloccare la navigazione su categorie e/o singoli siti i cui contenuti sia ritenuto come certamente estraneo agli interessi ed alle attività aziendali.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

- L'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentita la navigazione in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
- E' consentita l'effettuazione di transazioni finanziarie, ivi comprese le operazioni di remote banking, acquisti on-line e simili, solo per ridotti intervalli temporali o se espressamente autorizzati dall'ente;
- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- Non è permessa, se non autorizzata, la partecipazione a forum o chat, utilizzando pseudonimi (o nicknames);

3 *Indirizzo MAC (in inglese MAC address, dove MAC sta per Media Access Control), detto anche indirizzo fisico, indirizzo ethernet o indirizzo LAN, in informatica e telecomunicazioni, è un codice di 48 bit (6 byte) assegnato in modo univoco dal produttore ad ogni scheda di rete ethernet o wireless prodotta al mondo.*

4 *Indirizzo IP (dall'inglese Internet Protocol address) è un numero che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete per l'instradamento/indirizzamento.*

- Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica;
- È consentito l'utilizzo di soluzioni di Instant Messenger o chat esclusivamente per scopi professionali e attraverso strumenti e software messi a disposizione dall'ente;
- Non è consentito l'utilizzo o l'accesso a sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
- Non è consentita la condivisione e la fruizione di qualsiasi materiale anche se non protetto da copyright, utilizzando sistemi Peer-to-Peer, a qualsiasi titolo e anche se non a scopo di lucro.
- Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata preventivamente ed espressamente autorizzata.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere, in qualunque modo, nocivo all'immagine dell'ente.
Per mezzo della U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici e al fine di facilitare il rispetto delle sopra riportate regole, l'ente si riserva la facoltà di configurare filtri che inibiscano l'accesso a contenuti non consentiti e che prevengono operazioni non correlate all'attività lavorativa, a titolo esemplificativo e non esaustivo upload, restrizione nella navigazione, download di file o software.

Art. 12 – Gestione e utilizzo della posta elettronica aziendale

12.1 – Princìpi Guida

Per ciascun utente, ove previsto, l'ente provvede ad assegnare una casella di posta elettronica individuale del tipo: nome.cognome@izslt.it. La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", pertanto, i servizi di posta elettronica devono essere utilizzati a scopo professionale: l'account e-mail è uno strumento di proprietà dell'ente ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.
Ogni utente, ove previsto, ha la possibilità di accedere a caselle di posta elettronica condivise con altri utenti dello stesso gruppo/struttura (es. sistemi.informatici@izslt.it).
Attraverso le caselle e-mail aziendali gli utenti rappresentano pubblicamente l'ente e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine aziendale.
Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale conformemente alle presenti regole. Gli stessi devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (agenti di alterazione, ad esempio virus);
- Inviare preferibilmente files in formato PDF;
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo;
- rispondere alle e-mail pervenute solo da mittenti conosciuti o affidabili e cancellare le altre;
- collegarsi a siti internet contenuti all'interno di messaggi (click su link) solo per motivate ragioni e quando vi sia comprovata sicurezza sul contenuto degli stessi;
- mantenere in ordine la casella stessa, cancellando documenti inutili e soprattutto allegati ingombranti. È previsto un dimensionamento massimo per ciascuna casella in relazione alla

disponibilità di spazio dei sistemi di posta di volta in volta disponibili che non potrà essere superato.

Inoltre, non è consentito agli utenti:

- diffondere il proprio indirizzo e-mail aziendale attraverso la rete internet;
- utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'ente, per esempio presentazioni o materiali video aziendali;
- inviare catene telematiche (o di "Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo si deve procedere alla loro immediata cancellazione, non aprendo gli allegati ai tali messaggi;
- eseguire o favorire pratiche di spamming;
- utilizzare la casella di posta elettronica aziendale per iscrizioni a siti e/o servizi che ricadano nell'ambito della sfera privata dell'utente (società di erogazione energia, siti di e-commerce, siti di informazione, mostre e fiere non attinenti all'attività lavorativa, etc.).

Salvo l'utilizzo di appositi strumenti di cifratura i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale". E' preferibile, infine, che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute da altri nell'organizzazione di appartenenza del mittente.
Le presenti disposizioni si applicheranno anche agli account di Posta Elettronica Certificata.
Per la gestione della password della posta elettronica si rimanda al punto 7.2.

12.2 – Accesso alla casella di posta elettronica del lavoratore assente

Saranno messe a disposizione di ciascun utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che in caso di assenze programmate consentano di inviare automaticamente messaggi di risposta contenenti le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.
In caso di assenze non programmate, qualora il lavoratore non possa attivare la procedura descritta anche avvalendosi di servizi webmail da remoto e perdurando l'assenza oltre il limite temporale di 7 (sette) giorni l'ente potrà disporre, mediante il personale della U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici l'attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento).
Nel caso in cui l'ente necessiti di conoscere il contenuto dei messaggi di posta elettronica dell'utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

- la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato per iscritto dall'utente assente;
- di tale attività sarà redatto apposito verbale e informato l'utente interessato alla prima occasione utile.

12.3 – Cessazione dell'indirizzo di Posta Elettronica Aziendale

In caso di interruzione del rapporto di lavoro con l'utente, l'indirizzo di posta elettronica verrà disabilitato ed entro 30 (trenta) giorni dalla data della formale comunicazione del Direttore della UOC Risorse Umane e Affari Legali al Direttore dell'U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e

Informatica che disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'ente si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie attività.

Capo V — SANZIONI, COMUNICAZIONI, APPROVAZIONE

Art. 13 – Sanzioni

La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli art. 2104 e 2105 c.c., può comportare l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni disciplinari in base a quanto previsto dall'art. 7 (sanzioni disciplinari) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).
Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata l'ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali. In caso di violazione accertata delle regole e degli obblighi esposti in questo regolamento da parte degli utenti l'ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

Art. 14 – Informative

14.1 – Informativa agli utenti ex art. 13 Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati)

Il presente regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali e relativamente al trattamento di dati personali svolti dall'ente, così come definiti sopra, vale quale informativa ex art. 13 del Regolamento (UE) 2016/679.

14.2 – Informativa ai sensi dell'art. 13 del D.lgs. 196/2003 (Codice in materia di protezione dei dati personali)

Il Titolare del trattamento dei dati personali della presente direttiva è l'Istituto Zooprofilattico Sperimentale del Lazio e della Toscana *M. Aleandri*.
I Responsabili del trattamento dei dati personali vengono nominati dal Direttore Generale e pubblicati sul portale Aziendale.
I diritti previsti dall'art. 7 D.lgs. 196/2003 e in particolare il diritto di conoscere i dati che riguardano l'utente, il diritto di aggiornarli e il diritto di cancellare i dati eventualmente trattati in violazione di legge potranno essere esercitati rivolgendosi al Responsabile dei trattamenti, oppure al Titolare.

Art. 15 – Comunicazioni e autorizzazioni

Il presente regolamento è messo a disposizione degli utenti per la consultazione, in quanto adottato con delibera. Al fine di diffusione massimizzarne la diffusione e di dare la possibilità agli utenti di accedere sempre all'ultima versione di questo regolamento, lo stesso verrà pubblicato, dalla UOC Qualità, anche nell'area privata del sito istituzionale.
Al fine di rendere questo regolamento quanto più possibile aderente alla realtà aziendale e per garantire un veloce e costante suo aggiornamento, le eventuali successive revisioni verranno pubblicate, dalla UOC Qualità, nell'area privata del sito istituzionale anche senza adottarle attraverso uno specifico atto deliberativo. Gli aggiornamenti del presente regolamento verrà effettuati in analogia alle regole aziendali della qualità.
Gli utenti sono tenuti a conformarsi alle prescrizioni riportate nella revisione più aggiornata.

Le richieste di intervento e autorizzazione, previste nel presente regolamento, devono essere inoltrate dai dirigenti di struttura o da un loro delegato per mezzo di apposito sistema di ticketing che ne garantisca la tracciabilità e a cui è riconosciuto il valore di autorizzazione in forma scritta.

Il Direttore della U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici può non dare corso alle richieste d'intervento e autorizzazione inviate dai Dirigenti o dal loro delegato nel caso siano in contrasto con le disposizioni del presente regolamento o per motivazioni di tipo tecnico.

15.1 - Il Delegato

A supporto della propria attività, in relazione alle richieste di autorizzazione o concessione, previste dal presente regolamento, apertura e gestione dei ticket, ogni Responsabile di Unità può nominare un suo Delegato, richiedendo le eventuali credenziale di accesso al sistema di ticketing alla U.O.C. Tecnico Patrimoniale, Ingegneria Clinica e Sistemi Informatici.
Il delegato esegue le veci del Dirigente e nell'effettuare le richieste come nel rilasciare le autorizzazioni di cui al presente regolamento, assume su di sé il ruolo, le funzioni e le responsabilità del dirigente di struttura.

Art. 16 – Approvazione del Regolamento

Il presente regolamento è stato approvato dal Legale Rappresentante dell'ente attraverso un apposito e dedicato atto deliberativo.

Note conclusive

L'unico allegato al presente regolamento è costituito dal "Verbale di consegna e presa in carico di risorse informatiche".