# REGOLAMENTO DI SICUREZZA INFORMATICA PER PERSONALE ESTERNO

Teramo, 30 Giugno 2023

## CRONOLOGIA REVISIONI E SINTESI MODIFICHE

### Cronologia revisioni:

| Rev. | Data | Descrizione |
|---|---|---|
| 0 | 30.06.2023 | Il Regolamento riporta le prescrizioni relative all'utilizzo delle risorse informatiche e telematiche a cui si deve attenere il personale esterno che svolge la sua attività lavorativa, anche saltuaria, presso l'Istituto. |

### Sintesi delle modifiche rispetto alla precedente versione:

| Rev. | Descrizione |
|---|---|
| | |
| | |
| | |
| | |

# INDICE

NORMATIVA DI RIFERIMENTO ..... 4

AMBITO DI APPLICAZIONE E PRINCIPI ..... 5

Art. 1 - Introduzione ..... 5

Art. 2 - Ambito di applicazione ..... 5

Art. 3 - Principi Generali ..... 5

ACCESSO AL SISTEMA INFORMATICO ..... 7

Art. 4 - Credenziali di autenticazione ..... 7

Art. 5 - Gestione dei File ..... 8

DISPOSITIVI INFORMATICI ..... 9

Art. 6 - Personal Computer aziendale ..... 9

Art. 7 - Supporti rimovibili ..... 10

Art. 8 - Protezione da virus e da malware ..... 10

Art. 9 - Personal Computer non aziendale ..... 11

RETE INTERNET ..... 12

Art. 10 - Regole di utilizzo ..... 12

SOCIAL MEDIA ..... 13

Art. 11 - Prescrizioni ..... 13

GESTIONE DEGLI INCIDENTI DI SICUREZZA IT ..... 13

Art. 12 - Prescrizioni ..... 13

SISTEMA DEI CONTROLLI ..... 14

Art. 13 - Finalità e modalita' di esecuzione ..... 14

DISPOSIZIONI FINALI ..... 15

Art. 14 - Sanzioni ..... 15

Art. 15 - Aggiornamento e Revisione ..... 15

Art. 16 - Entrata in vigore e diffusione ..... 15

# NORMATIVA DI RIFERIMENTO

- D. Lgs. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”;
- Regolamento (EU) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - GDPR)”;
- D. Lgs. 10 agosto 2018, n. 101 recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”;
- D. Lgs. 7 marzo 2005, n. 82 “Codice dell’Amministrazione Digitale”;
- Linee guida e provvedimenti specifici del Garante per la Protezione dei Dati Personali;

## Titolo I

# AMBITO DI APPLICAZIONE E PRINCIPI

### ART. 1 - INTRODUZIONE

Il presente **Regolamento di Sicurezza informatica per il personale esterno** (di seguito "**Regolamento esterni**") riporta le prescrizioni relative all'utilizzo delle risorse informatiche e telematiche a cui si devono attenere le persone (di seguito "**Personale Esterno**") che, a fronte di un contratto di collaborazione formalizzato e sottoscritto, devono prestare la propria attività lavorativa, anche saltuaria, presso l'*Istituto Zooprofilattico Sperimentale dell'Abruzzo e del Molise "G. Caporale"* (di seguito "**Istituto"**).

Il presente **Regolamento**, nel rispetto delle vigenti disposizioni normative in tema di protezione dei dati personali e strumenti di controllo, ha altresì lo scopo di informare il *Personale Esterno* – ai sensi dell'art. 12 e ss del Regolamento Europeo 2016/679 - sulle eventuali finalità e modalità dei controlli riferiti all'utilizzo degli strumenti informatici e sulle specifiche tecnologie adottate per effettuarli.

### ART. 2 - AMBITO DI APPLICAZIONE

Il presente **Regolamento Esterni** si applica a tutto il *Personale Esterno*, senza distinzione di ruolo o di mansione.

Si precisa che tutto quanto non espressamente autorizzato ai sensi del presente **Regolamento Esterni** è da ritenersi vietato.

Il *Personale Esterno* è coordinato da specifici **Referenti Aziendali** a cui è tenuto rivolgersi per qualsiasi chiarimento o richiesta nell'applicazione del presente **Regolamento Esterni**.

### ART. 3 - PRINCIPI GENERALI

L'utilizzo delle risorse informatiche e telematiche, nell'ambito del rapporto contrattuale, deve sempre ispirarsi ai principi di diligenza e correttezza.

L'*Istituto* ha adottato il presente **Regolamento Esterni** diretto a fornire le prescrizioni per il corretto utilizzo dell'ambiente informatico aziendale ed evitare comportamenti che possano indurre problemi o minacce alla Sicurezza IT in generale.

Il mancato rispetto delle prescrizioni di sicurezza contenute nel presente **Regolamento Esterni** costituisce violazione dell'obbligo contrattuale.

L'utilizzo delle risorse informatiche e telematiche è consentito al *Personale Esterno* solo per finalità di adempimento delle mansioni assegnate.

Sono vietati comportamenti che possano creare un danno, anche di immagine, all'*Istituto*.

Il *Personale Esterno* deve utilizzare gli strumenti informatici e telematici rispettando le seguenti regole di comportamento:

a. non deve introdursi in sistemi informatici o telematici ai quali non sia autorizzato ad accedere, in particolare se l'indebita intromissione o permanenza riguarda sistemi informatici o telematici protetti da misure di sicurezza;

b. non deve utilizzare o mettere a disposizione abusivamente codici di accesso o password o altri mezzi, i quali consentono di accedere, in modo logico o fisico, a sistemi informatici o telematici protetti da misure di sicurezza;

c. non deve utilizzare gli strumenti di comunicazione (quali, ad esempio, Internet o reti telematiche in genere) per offendere l'onore, il decoro o la reputazione di altre persone.

Al *Personale Esterno*, in casi specifici, può essere concesso l'utilizzo di dispositivi elettronici non aziendali esclusivamente per accedere ad Internet, con le modalità previste dall'*Art. 9 - Personal Computer non aziendali*.

L'*Istituto*, in linea con quanto prescritto dall'ordinamento giuridico italiano, esclude la configurabilità di forme di controllo aventi direttamente ad oggetto l'attività lavorativa dell'utente. Tuttavia non si esclude che, per esigenze dettate dalla sicurezza del lavoro, dall'utilizzo di sistemi informatici, impianti, apparecchiature o dispositivi possa derivare la possibilità di controllo a distanza dell'attività svolta. In tal caso, tali strumenti verranno valutati e subordinati rispetto alla normativa di settore.

## Titolo II

# ACCESSO AL SISTEMA INFORMATICO

### ART. 4 - CREDENZIALI DI AUTENTICAZIONE

L'accesso al Personal Computer aziendale e alla Rete Aziendale è protetto da credenziali (*userid e password*) consegnate al *Personale Esterno* dal **Reparto Gestione Telematica** e costituite da un codice identificativo dell'utente (*userid*) associato ad una parola chiave (*password*) che consente di verificarne l'identità.

L'accesso ad una Applicazione può essere protetto da ulteriori credenziali, che possono essere identiche o diverse da quelle di accesso al Personal Computer e alla Rete Aziendale. Qualora diverse, devono sottostare ai vincoli previsti dall'Applicazione e che, se necessarie, saranno consegnate al *Personale Esterno* dal **Responsabile dell'Applicativo**.

Relativamente alle credenziali di accesso al Personal Computer e alla Rete Aziendale, valgono le seguenti prescrizioni:

a. al *Personale Esterno* sono assegnate le pertinenti credenziali di autenticazione il cui corretto utilizzo è obbligatorio per l'accesso all'ambiente di lavoro dell'*Istituto*;

b. la *password* iniziale, assegnata in occasione del primo accesso, deve essere immediatamente modificata ad esclusiva cura dell'assegnatario, e successivamente deve essere obbligatoriamente modificata con la periodicità e le modalità previste;

c. la composizione della *password* deve seguire le regole previste, richieste e controllate dallo specifico software acceduto, ed in particolare non deve coincidere con una sequenza banale di caratteri (ad es. 12345678), e non deve contenere riferimenti facilmente riconducibili all'Utente (ad es. data di nascita, nome, cognome, nome dell'azienda, ecc.). Il Sistema Informativo è configurato per controllare automaticamente la robustezza della *password* e per richiederne il cambio alla sua scadenza;

d. la *password*, in particolare, non deve coincidere con quella abitualmente utilizzata per l'accesso ad altri sistemi esterni all'Istituto;

e. le credenziali (*userid* e *password*) sono strettamente personali, ovvero associate univocamente alla persona assegnataria, devono essere custodite con la massima diligenza e non devono essere rivelate ad alcuno per nessun motivo;

f. la *password* non deve essere memorizzata su file, appunti, post-it, etc …, e deve essere digitata ogni volta*;*

g. nel caso di sospetto che altri possano essere venuti a conoscenza della propria *password*, il *Personale Esterno* dovrà procedere immediatamente alla modifica della stessa e, contestualmente, segnalare l'evento (vedi *Capo IV - Gestione degli Incidenti di Sicurezza IT*) per gli interventi del caso.

Qualora, in funzione della criticità dei dati trattati e/o delle abilitazioni attribuite, vengano utilizzati sistemi di autenticazione a due fattori, il *Personale Esterno* deve adeguarsi alle

disposizioni che gli verranno di volta in volta impartite.

In casi del tutto eccezionali, l'*Istituto* si riserva la possibilità di utilizzare l'utenza del *Personale Esterno*, tramite la forzatura delle credenziali di accesso. Tale forzatura avviene esclusivamente nei casi e con le modalità previste nella specifica Procedura che, tra l'altro, prevede l'avviso al *Personale Esterno* oltre alla tracciatura delle autorizzazioni date e delle attività svolte.

## ART. 5 - GESTIONE DEI FILE

Il *Personale Esterno***,** può essere autorizzato, in base all'attività assegnata, ad accedere e/o gestire *file* su determinate *cartelle di rete,* posizionate sui *server* o sulle *risorse cloud* dell'*Istituto*.

In questo caso, valgono le seguenti prescrizioni:

a. le *cartelle 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, su di esse;

b. le *cartelle di rete* vengono accedute in base alle abilitazioni attribuite al *Personale Esterno*;

c. le *risorse cloud* devono essere accedute esclusivamente con le modalità specificamente predisposte in funzione della tipologia di risorsa. Per i dati memorizzati su tali risorse, il Fornitore del servizio cloud mantiene il backup delle diverse versioni, consentendone il recupero quando necessario;

d. l'archiviazione di *file* di lavoro su cartelle locali (cartelle presenti nel PC assegnato) è consentita solo per brevi periodi, pari al tempo strettamente necessario per eseguire operazioni per cui sia necessaria tale archiviazione;

*e.* la responsabilità del salvataggio dei file su cartelle locali è a carico del *Personale Esterno;*

f. è vietata in ogni caso l'archiviazione, nel PC assegnato, di *file* con dati personali.

Sui *server* che ospitano le *cartelle di rete* vengono svolte dall'*Amministratore di Sistema* regolari attività di controllo e di amministrazione ed in particolare sono previsti periodici salvataggi dei dati (*backup)* secondo quanto previsto dalle specifiche Procedure.

Il personale tecnico con qualifica di *Amministratore di Sistema* può, in qualunque momento, procedere alla rimozione d'ufficio di elementi (*file* o *cartelle*) ritenuti pericolosi per la sicurezza dell'ambiente di lavoro, presenti su cartelle di rete, cartelle locali e cartelle in Cloud.

**Titolo III**
**Capo I**

# DISPOSITIVI INFORMATICI

## ART. 6 - PERSONAL COMPUTER AZIENDALE

Nel caso in cui l'*Istituto* metta a disposizione del *Personale Esterno* un Personal Computer (PC) fisso o portatile, valgono le prescrizioni che seguono:

a. Il PC deve essere custodito con cura evitando ogni possibile forma di danneggiamento;
b. il PC è uno strumento di lavoro, non è consentito in alcun modo un utilizzo per scopi personali e non è consentita l'archiviazione su di esso di dati personali;
c. il PC viene fornito già predisposto e opportunamente configurato per permettere di assolvere alle attività lavorative previste;
d. non è consentita la modifica delle configurazioni impostate sul PC assegnato né la reinstallazione o alterazione del sistema operativo o di qualsiasi altro software in dotazione;
e. non sono consentiti l'installazione e l'uso di *software* diversi da quelli in dotazione, ufficialmente installati e preventivamente autorizzati dall'*Istituto*;
f. è fatto divieto assoluto di formattare o alterare o manomettere o distruggere il PC assegnato o rendere inintelligibili i dati in essi contenuti;
g. il PC deve essere posto in modalità manuale di blocco (*screen saver*) in caso di non utilizzo (ad es. breve allontanamento) e comunque deve essere spento a fronte di assenze prolungate (ad es. uscita serale dall'ufficio).

Qualora fosse necessario utilizzare un *software* differente da quello in dotazione o disporre di una configurazione diversa per il PC assegnato, il *Personale Esterno* provvede ad inoltrare una specifica richiesta all'Helpdesk IT e per conoscenza al proprio Referente Aziendale. Richiesta che seguirà il flusso di approvazione previsto relativamente agli aspetti di opportunità, sicurezza e scelta tecnologica.

Relativamente ai PC portatili, il *Personale Esterno* dipendente è tenuto a custodirlo con la massima diligenza sia durante l'utilizzo nel luogo di lavoro, sia al di fuori del luogo di lavoro o durante trasferte o spostamenti, adottando tutte le cautele necessarie per evitare danni o sottrazioni di dati, documenti o informazioni presenti nel PC stesso.
Al riguardo i veicoli (privati, aziendali, a noleggio, etc.) devono essere considerati come "luoghi insicuri" e pertanto i dispositivi portatili non devono essere lasciati incustoditi all'interno di essi, anche nel caso in cui non siano visibili dall'esterno (ad es. riposti nel bagagliaio).

Nel caso di perdita, smarrimento o furto del dispositivo portatile assegnato, il *Personale Esterno* deve avvertire immediatamente il proprio Referente Aziendale e il Reparto Gestione

Telematica e, qualora ne ricorrano le circostanze, deve immediatamente denunciare l'evento alle Forze dell'Ordine e consegnare copia della verbalizzazione.

L'*Istituto* si riserva il diritto di sospendere l'utilizzo del PC qualora non sia più necessario all'esecuzione delle attività previste, al termine del rapporto contrattuale o a fronte di un utilizzo non conforme al presente **Regolamento Esterni**. In tutti questi casi è fatto obbligo al **Personale Esterno** di procedere immediatamente alla restituzione del PC assegnato.

Al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro *virus, spyware*, *malware*, ecc., il personale tecnico con qualifica di "*Amministratore di Sistema*" può avere la necessità di collegarsi anche da remoto al PC a seguito di specifica richiesta del *Personale Esterno* che deve autorizzarlo. Comunque, in caso di oggettiva necessità – e cioè a seguito di problematiche tecniche rilevate e rischiose rispetto alla rete e/o ai sistemi informativi dell'*Istituto* – il personale tecnico incaricato, autorizzato dal **Responsabile Gestione Telematica**, potrà intervenire direttamente, al fine di non pregiudicare la necessaria immediatezza ed efficacia dell'intervento, fornendo al *Personale Esterno* tempestiva comunicazione dell'avvenuto accesso.

## ART. 7 - SUPPORTI RIMOVIBILI

L'*Istituto* non ammette per il *Personale esterno* l'utilizzo di supporti rimovibili, come ad es. chiavette USB, hard disk esterni, SD card, … salvo specifica autorizzazione del **Responsabile Gestione Telematica** che comunicherà le opportune istruzioni cui attenersi.

## ART. 8 - PROTEZIONE DA VIRUS E DA MALWARE

Il Sistema Informatico dell'*Istituto* è protetto da *software* antivirus mantenuto periodicamente aggiornato. Comunque il *Personale Esterno* deve mettere in atto comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante *virus* o mediante ogni altro *software* aggressivo (*malware*).

In particolare valgono le seguenti prescrizioni:

a. è fatto assoluto divieto di disinstallare, modificare le impostazioni o disattivare anche solo temporaneamente l'antivirus, in quanto pericoloso per il proprio Personal Computer e per l'intera Rete Aziendale;

b. nel caso in cui il *software* antivirus rilevi la presenza di un virus, il *Personale Esterno* deve sospendere immediatamente ogni elaborazione in corso, scollegare il PC dalla rete evitando ove possibile di spegnerlo, nonché segnalare prontamente l'evento al **Reparto Gestione Telematica** (vedi *Capo IV - Gestione degli Incidenti di Sicurezza IT*).

## ART. 9 - PERSONAL COMPUTER NON AZIENDALE

L'*Istituto* ammette, in casi particolari e specificamente autorizzati o regolati dal rapporto contrattuale, la presenza nelle proprie sedi di *Personale Esterno* dotato di Personal Computer (PC) non di proprietà aziendale.

In questo caso valgono le prescrizioni che seguono:

a. non è permesso l'accesso alla Rete Interna dell'*Istituto*, salvo espressa autorizzazione concessa dal **Responsabile Sicurezza IT**;

b. è permessa esclusivamente l'uscita in Internet con modalità regolate dalla normativa aziendale (si veda in particolare il *Capo II – RETE INTERNET – ART.10 Regole di Utilizzo*), e solo per fini lavorativi;

c. il *Personale Esterno* deve svolgere solo le attività consentite ed evitare qualsiasi azione o comportamento che possa esporre all'esterno dati e/o documenti dell'*Istituto* e/o informazioni soggette a *privacy*.

Qualora fossero necessarie differenti modalità di utilizzo, il *Personale Esterno* deve rivolgersi al proprio **Referente Aziendale** che, se del caso, provvede ad inoltrare specifica richiesta al **Responsabile Sicurezza IT** e a comunicare al *Personale Esterno* le eventuali istruzioni cui attenersi e gli impegni da sottoscrivere.

## Capo II

# RETE INTERNET

### ART. 10 - REGOLE DI UTILIZZO

Il *Personale Esterno***,** può essere autorizzato, in base all'attività svolta, ad accedere alla "*navigazione Internet*".

Il *Personale Esterno* deve essere consapevole che l'utilizzo improprio di questo servizio può avere conseguenze, anche rilevanti, in termini d'immagine dell'*Istituto*, di etica dell'ambiente di lavoro e di sicurezza dei sistemi informatici, e potrà essere chiamato a risponderne.

Al fine di evitare la navigazione in siti non pertinenti con l'attività lavorativa o a rischio di sicurezza, l'*Istituto* predispone specifichi blocchi o filtri automatici che prevengono operazioni quali l'*upload* e/o l'accesso a determinati siti inseriti in una *black list*.

Valgono le seguenti prescrizion**i**:

a. la navigazione in Internet è riservata allo svolgimento dell'attività lavorativa e non deve essere utilizzata a fini personali;
b. non si deve effettuare l'*upload* o il *download* di software, nemmeno se gratuiti (*freeware*) o liberamente utilizzabili (*shareware*);
c. non si devono utilizzare documenti o file (filmati e/o musica) provenienti da siti web, se non strettamente attinenti all'attività lavorativa;
d. non si deve accedere a connessioni anonime che non consentano l'identificazione dell'indirizzo di navigazione;
e. non si devono svolgere attività in contrasto con le disposizioni di legge.

Qualora, per particolari esigenze lavorative, il *Personale Esterno* debba accedere a determinati siti inclusi nella *black list*, quest'ultimo può rivolgersi al proprio **Referente Aziendale** che, se del caso, provvederà a richiedere specifica abilitazione al **Reparto Gestione Telematica**.

I *log* di accesso alla rete internet e i *log* di navigazione, in accordo con le disposizioni di legge vigenti, vengono mantenuti per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'*Istituto*. È in ogni caso osservato il principio di pertinenza temporale del trattamento, in modo che la tenuta dei dati sia effettivamente congrua e giustificabile alla luce delle esigenze tecniche di gestione del sistema informatico.

L'accesso ai *log* suddetti avviene esclusivamente nei casi e con le modalità previste nella specifica Procedura. Tale controllo non è continuativo, ma viene posto in essere solo in presenza di anomalie e viene effettuato inizialmente sulla base di informazioni anonime e aggregate, intervenendo in modo più accurato solo qualora circostanze oggettive e documentate ne giustifichino la necessità, applicando il sistema dei controlli graduali (vedi *Capo V - Sistema dei controlli*).

## Capo III

# SOCIAL MEDIA

### ART. 11 - PRESCRIZIONI

Il *Personale Esterno* non può divulgare attraverso i Social Media contenuti o eventi dell'*Istituto* se non specificamente autorizzato dal proprio **Referente Aziendale** che comunicherà le opportune istruzioni cui attenersi.

## Capo IV

# GESTIONE DEGLI INCIDENTI DI SICUREZZA IT

### ART. 12 - PRESCRIZIONI

Gli **Incidenti di Sicurezza IT**, intesi come eventi che possano compromettere la Sicurezza dell'*Istituto* (in particolare eventi di *CyberSecurity*), si verificano sempre più frequentemente e l'*Istituto* è consapevole della minaccia.

Per una risposta efficace è importante una reazione rapida da parte del *Personale Esterno* e per questo è necessario riconoscere tempestivamente un potenziale **incidente di sicurezza IT**, come ad esempio la:

- segnalazione della presenza di un possibile virus;
- rilevazione di una situazione insolita o inattesa (ad es. una password disabilitata senza un motivo apparente);
- rilevazione di comportamenti insoliti del PC (ad es. continui riavvii);
- richiesta insistente di informazioni personali senza un valido motivo.

Per il *Personale Esterno* vale la prescrizione che segue:

a. qualora venga a conoscenza di un potenziale **Incidente di Sicurezza IT** deve informare immediatamente il **Reparto Gestione Telematica** e contestualmente il proprio **Referente Aziendale**.

## Capo V

# SISTEMA DEI CONTROLLI

### ART. 13 - FINALITÀ E MODALITA' DI ESECUZIONE

Si ricorda che sugli strumenti elettronici utilizzati, sui server acceduti e sui firewall rimangono sempre tracce delle attività svolte (*Log*).

L'*Istituto*, nel rispetto del divieto di utilizzo di strumenti tecnologici preordinati al controllo dell'attività lavorativa, assicura che strumenti tecnologici di controllo potranno essere installati, se del caso, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e/o per la tutela del patrimonio, e per tutte le finalità previste dal rapporto contrattuale, previa idonea informativa all'interessato.

Eventuali controlli, che in nessun caso saranno prolungati, costanti o indiscriminati, potranno avvenire con modalità di *controlli graduali*, come di seguito definito:

**A.** **Controlli generalizzati**: in caso di anomalie o malfunzionamenti, il personale incaricato effettuerà, mediante l'ausilio dei sistemi installati, controlli anonimi che si concluderanno con avvisi generalizzati diretti a tutti gli utenti. I suddetti avvisi evidenzieranno i comportamenti rilevati non conformi alle prescrizioni e inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite.

**B.** **Controlli su base individuale**: in caso di persistenza dell'anomalia, successivamente all'invio dell'avviso generalizzato, il personale incaricato potrà effettuare interventi mirati seguendo comunque procedure definite allo scopo.

Controlli su base individuale potranno comunque venire effettuati in via eccezionale e tassativa, oltre che nell'ipotesi sopra menzionata, anche ove ricorra una o più delle seguenti ipotesi**:**

- quando venga presentata una specifica richiesta di informazioni da parte dell'Autorità giudiziaria;
- quando si verifichi un evento dannoso o una situazione di pericolo che richiedano un immediato e necessario intervento.

I dati raccolti dai predetti controlli potranno essere utilizzati per tutte le finalità connesse al rapporto contrattuale, nel rispetto della normativa *Privacy*.

## Titolo IV

# DISPOSIZIONI FINALI

### ART. 14 - SANZIONI

È fatto obbligo al *Personale Esterno* di adeguarsi a quanto richiesto dal presente **Regolamento Esterni**, in quanto ogni comportamento non conforme ad esso espone l'*Istituto* ad eventuali danni patrimoniali e/o penali che possono compromettere la sicurezza e l'immagine dell'*Istituto.*

Il mancato rispetto o la violazione le disposizioni contenute nel presente **Regolamento Esterni** è perseguibile secondo quanto previsto dal rapporto contrattuale e, verificata la gravità della violazione contestata, anche con la risoluzione o il recesso dal contratto, nonché con tutte le azioni civili e penali consentite.

### ART. 15 - AGGIORNAMENTO E REVISIONE

Il presente **Regolamento Esterni** è soggetto a revisione periodica, almeno annuale e comunque in caso di modifiche dei processi e delle *policy* dell'*Istituto*.

La versione aggiornata del **Regolamento Esterni** è disponibile nella Sezione Regolamenti Esterni sulla Bacheca presente sulla Intranet aziendale.

A fronte di modifiche del **Regolamento Esterni,** i singoli **Referenti Aziendali** che hanno in carico il *Personale Esterno* dovranno provvedere all'informativa e a raccogliere nuova sottoscrizione.

### ART. 16 - ENTRATA IN VIGORE E DIFFUSIONE

Il presente **Regolamento di Sicurezza Informatica per il personale esterno** entra in vigore a partire dalla data di emissione sotto riportata.

Con l'entrata in vigore del **Regolamento Esterni** tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Il presente **Regolamento di Sicurezza Informatica per il personale esterno** viene comunicato per sottoscrizione ai singoli soggetti interessati dai rispettivi **Referenti Aziendali** ed integra il rapporto contrattuale.

Data di emissione: 30/06/2023