MINISTERO DELL' ISTRUZIONE DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO "VIA BOCCEA 590"
Via Boccea, 590 - 00166 Roma Tel. 06/61568029 - Fax 06/61567511
Distretto XXVI - Municipio XIII
Codice Fiscale 97200630586 - Codice Scuola RMIC84400N
e-mail : rmic84400n@istruzione.it
e-mail : rmic84400n@pec.istruzione.it
www.icviaboccea590.gov.it

All'amministratore di sistema Sig Giovanni Rizzo
S.r.l. BLIXEN

All'albo dell'Istituto SEDE

DESIGNAZIONE DELL'AMMINISTRATORE DI SISTEMA

IL DIRIGENTE SCOLASTICO

VISTO il Regolamento generale sulla protezione dei dati, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, d'ora in poi "Regolamento";
Le "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" - 27 novembre 2008 del Garante per la protezione dei dati personali, modificati in base al provvedimento del 25 giugno 2009,

PREMESSO CHE titolare del trattamento è l'istituto stesso, di cui il dirigente scolastico è legale rappresentante pro-tempore,

CONSIDERATO CHE l'art. 24 del Regolamento impone al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento stesso;
l'art. 30 del Regolamento impone al titolare del trattamento la tenuta di un registro di tutte le categorie di attività relative al trattamento svolte per conto del titolare del trattamento;
l'art. 32 del Regolamento impone al titolare del trattamento l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio nel trattamento dei dati personali;
il trattamento dei dati personali viene eseguito anche con sistemi informatici,

RITENUTO CHE il soggetto da designare presenti garanzie, capacità ed esperienza adeguate:

1. alla gestione e alla trattazione informatica dei dati personali;
2. a garantire la sicurezza dei sistemi informatici;
3. a garantire la protezione dei dati sin dalle fasi di progettazione e per impostazione predefinita (privacy by design e privacy by default di cui all'art. 25 del Regolamento),

DESIGNA

il Sig Giovanni Rizzo BLIXEN S.r.l., con sede in via Emiliano Sarti 29 – 00124 Roma (RM), C.F./P. Iva 06864221004, quale

Amministratore di sistema e Responsabile del trattamento informatico

nell'ambito dell'organizzazione di questo istituto, affidandogli i seguenti compiti e responsabilità in aderenza a quanto contenuto nelle misure tecniche e organizzative – trattamenti con strumenti elettronici – previste ai sensi dell'art. 32 del Regolamento (Allegato 1 alla presente designazione), la cui inosservanza può determinare responsabilità risarcitorie, sanzionatorie e penali:

1. eseguire, all'inizio dell'incarico e con frequenza semestrale, un rilievo degli apparati di rete, server, postazioni di lavoro e dei collegamenti verso l'esterno;
2. garantire, da remoto o in loco, assistenza ai tecnici dell'istituto o la risoluzione dei problemi/inconvenienti riscontrati sulla rete, sui server e sulle postazioni di lavoro (postazione con personal computer o registro elettronico) entro 24 ore dalla richiesta di intervento;
3. gestire il sistema informatico, nel quale risiedono le banche dati personali, in osservanza alle misure di sicurezza previste all'art. 32 del Regolamento;
4. predisporre ed aggiornare un sistema di sicurezza informatico idoneo a rispettare le prescrizioni degli articoli 24 e 32 del Regolamento, nello specifico:
   a) assegnare e gestire il sistema di autenticazione informatica secondo le modalità indicate nell'Allegato 1 "trattamenti con strumenti elettronici" e quindi, fra le altre, procedere alla disattivazione delle credenziali in caso di perdita della qualità che consentiva all'incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo delle credenziali per oltre 6 (sei) mesi; la funzione di custode delle copie delle credenziali è svolta dal DSGA dott.ssa Maria Grazia PANACEA;
   b) adottare adeguati programmi antivirus, firewall e strumenti software e/o hardware atti a garantire il rispetto dei requisiti di sicurezza richiesti dal Regolamento, attraverso le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento;
   c) adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure attivate in struttura. L'amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
   d) provvedere, direttamente o per il tramite degli incaricati interessati, alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento degli strumenti elettronici;
   e) cooperare, con il titolare del trattamento e il responsabile della protezione dei dati, alla predisposizione delle misure tecniche di sicurezza per la parte concernente il sistema informatico ed il trattamento informatico dei dati;

f) vigilare sugli interventi diretti al sistema informatico dell'istituto effettuati, a qualsiasi titolo, da operatori esterni (ad es. società che forniscono servizi telematici a questo istituto). In caso di anomalie sarà cura dell'amministratore di sistema segnalarle direttamente al titolare del trattamento e al responsabile della protezione dei dati;

5. coordinare assieme al titolare e al responsabile del trattamento per la funzione "personale amministrativo" le attività operative degli incaricati al trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali nell'ambito del sistema informatico;
6. collaborare con il titolare del trattamento e il responsabile della protezione dei dati per l'attuazione delle prescrizioni impartite dal Garante della privacy;
7. comunicare prontamente al titolare del trattamento, al responsabile del trattamento per la funzione "personale amministrativo" e al responsabile della protezione dei dati qualsiasi situazione di cui sia venuto a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali;
8. verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaboratore installati nei computer presenti nell'istituto;
9. adottare e gestire sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di tutte le persone qualificate amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Per l'espletamento dell'incarico, vengono assegnate all'amministratore di sistema le credenziali di autenticazione che gli permettono l'accessibilità al sistema per lo svolgimento delle stesse funzioni assegnate.

A seguito di uno qualunque degli interventi elencati nella presente lettera, in qualità di soggetto esterno all'istituto, l'amministratore di sistema dovrà presentare al titolare del trattamento, per il tramite del responsabile della protezione dei dati, una **descrizione scritta dell'intervento effettuato** che ne attesti la conformità alle disposizioni di sicurezza adottate da questo istituto.

L'istituto provvederà a svolgere le dovute verifiche sulle attività compiute dall'amministratore di sistema. È obbligo di quest'ultimo prestare all'istituto la sua piena collaborazione per il compimento delle verifiche stesse. Nell'ambito dei compiti previsti dall'art. 39 del Regolamento, l'osservanza delle disposizioni in materia di protezione dei dati personali da parte dell'amministratore di sistema è sorvegliata dal Responsabile della protezione dei dati personali, nella persona dell'ing. Marco Magazzeni.

Della nomina ad amministratore di sistema, così disposta con il presente atto, verrà data opportuna informazione, nell'ambito dell'organizzazione dell'istituto, al personale interessato, attraverso espresso richiamo nell'informativa dei dati personali.

Gli allegati (Allegato 1: misure di sicurezza nei trattamenti con strumenti elettronici e Allegato 2: informativa per Ditte/lavoratori autonomi da somministrare all'interessato) sono parte integrante della presente designazione.

Forme di comunicazione, recapiti e individuazione referente
Amministratore di sistema: Sig Giovanni Rizzo BLIXEN S.r.l.
– cell. 339 6525981 – e-mail: info@blixen.it

Titolare del trattamento: Istituto Comprensivo via Boccea, 590, con sede legale in via Boccea, 590 - 00166 Roma, in persona del legale rappresentante Dirigente Scolastico Prof.ssa Ermenegilda ESPOSITO, PEC: rmic84400n@pec.istruzione.it.

Responsabile della protezione dei dati: Ing. Marco MAGAZZENI, e-mail: info@rlsicurezza.it – PEC: mmgformazione@legalmail.it.

Con la sottoscrizione della presente, l'Amministratore di sistema accetta la nomina, conferma altresì la diretta ed approfondita conoscenza della normativa in materia di protezione dei dati personali nonché degli obblighi in essa prevista.

il Titolare del trattamento
Dirigente Scolastico
Prof.ssa Ermenegilda ESPOSITO

Ermenegilda Esposito

Firmato digitalmente da Ermenegilda Esposito
ND: cn=Ermenegilda Esposito, o=IC Via Boccea 590, ou=Dirigente scolastico, email=ermenegilda.esposito@istruzione.it, c=IT
Data: 2018.11.20 12:26:06 +01'00'

l'Amministratore di sistema
BLIXEN S.r.l.
Sig Giovanni Rizzo

Allegato 1 alla lettera di designazione dell'amministratore di sistema

Misure tecniche e organizzative
(art. 32 del Regolamento)

Trattamenti con strumenti elettronici

Sistema di autenticazione informatica per il sistema operativo e i software di trattamento dati

1. **CREDENZIALI DI AUTENTICAZIONE**
   a) il trattamento dei dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti;
   b) le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo;
   c) ad ogni incaricato sono assegnate individualmente le credenziali per l'autenticazione. Le credenziali di autenticazione sono assolutamente **personali** e **non cedibili**, per nessuna ragione;
   d) sono disattivate se non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
   e) sono disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

2. **GLI INCARICATI DEVONO ADOTTARE LE NECESSARIE CAUTELE PER ASSICURARE LA SEGRETEZZA DELLA COMPONENTE RISERVATA DELLA CREDENZIALE E LA LORO DILIGENTE CUSTODIA**
   *In particolare gli incaricati **devono**:*
   a) utilizzare password distinte per sistemi con diverso grado di sensibilità. In alcuni casi le password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa da quella usata da sistemi "sicuri";
   b) porre in essere quanto riportato ai punti a), b), c) e d) relativi alla parola chiave,
   *mentre **non devono**:*
   a) comunicare ad altra persona la propria password (lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le proprie risorse o possa farlo a proprio nome);
   b) scrivere la propria password su fogli di carta che possono essere letti facilmente, ad esempio vicino al computer;
   c) immette la password quando c'è il rischio che qualcun altro possa leggere il contenuto sulla tastiera del

computer;
d) scegliere password che si possono trovare in un dizionario;
e) credere che usare parole straniere renda più difficile il lavoro di scoperta;
f) usare il proprio nome utente: è la password più semplice da indovinare;
g) usare password in qualche modo legate alla propria persona come, ad esempio, il proprio nome, quello della moglie/marito, dei figli, del cane, date di nascita, numeri di telefono, etc..

3. **LA PAROLA CHIAVE:**
   a) deve essere composta da almeno otto caratteri (nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito) e deve essere alfanumerica;
   b) non deve contenere riferimenti agevolmente riconducibili all'incaricato;
   c) è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi;
   d) in caso di trattamento di dati sensibili e giudiziari la parola chiave è modificata almeno ogni tre mesi.

4. **PER NON LASCIARE INCUSTODITO E ACCESSIBILE LO STRUMENTO ELETTRONICO DURANTE UNA SESSIONE DI TRATTAMENTO, GLI INCARICATI DEVONO SVOLGERE ALMENO UNA DELLE SEGUENTI OPERAZIONI**
   a) terminare la sessione di lavoro al computer ogni volta che ci si deve allontanare, effettuando un log out o mettendo in atto accorgimenti tipo il blocco della sessione;
   b) un collega, che abbia lo stesso profilo autorizzativo nel trattamento dei dati, deve rimanere nella stanza durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;
   c) chiudere a chiave la stanza dove è situato lo strumento elettronico durante l'assenza dell'incaricato, se nella stessa non rimane nessuno.
5. **MODALITÀ CON LE QUALI IL TITOLARE ASSICURA LA DISPONIBILITÀ DI DATI O STRUMENTI ELETTRONICI IN CASO DI PROLUNGATA ASSENZA O IMPEDIMENTO DELL'INCARICATO CHE RENDA INDISPENSABILE E INDIFFERIBILE INTERVENIRE PER ESCLUSIVE NECESSITÀ DI OPERATIVITÀ E DI SICUREZZA DEL SISTEMA**
   a) il soggetto incaricato della custodia delle copie delle credenziali di ciascun incaricato è il DSGA dott.ssa Maria Grazia PANACEA;
   b) per ciascun incaricato, la copia delle credenziali deve essere conservata in **busta chiusa munita di data, firma e sigillo** apposto direttamente dall'incaricato proprietario delle credenziali stesse;
   c) le buste sono conservate in contenitore chiudibile a chiave, collocato a sua volta nell'armadio blindato dell'ufficio del DSGA;
   d) in caso di assenza di un incaricato e di necessità ad operare un trattamento in sua vece, il DSGA autorizza l'apertura della busta e assegna l'operatività ad altro incaricato; contestualmente verrà data comunicazione all'interessato assente di quanto accaduto. Al ritorno di quest'ultimo, verrà ripristinata l'operatività originaria dopo che l'incaricato avrà rielaborato una nuova password e consegnato una copia delle credenziali aggiornate al DSGA.

6. **I DATI PERSONALI SONO PROTETTI CONTRO IL RISCHIO DI INTRUSIONE E DELL'AZIONE DI PROGRAMMI DI CUI ALL'ART. 615-QUINQUIES DEL CODICE PENALE, MEDIANTE L'ATTIVAZIONE DI IDONEI STRUMENTI ELETTRONICI DA AGGIORNARE CON CADENZA ALMENO SEMESTRALE**
   1. i computer sono protetti dal programma antivirus **Microsoft Security Essentials** che è un antivirus freeware creato da Microsoft che difende i computer da virus, spyware, rootkit e trojan;
   2. il programma antivirus viene aggiornato con cadenza **almeno trimestrale**;
   3. la rete informatica e i programmi e applicativi che trattano dati sensibili e giudiziari sono protetti contro l'accesso abusivo ai sensi dell'art. 615-ter del Codice Penale attraverso l'installazione di idonei dispositivi elettronici (firewall e programmi denominati Intrusion Detection System, IDS).

Linee guida per la prevenzione dei virus informatici

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido o a catturare

informazioni riservate (password/chiavi di sblocco, etc.).

Comportamenti che aumentano il rischio di contrarre un virus informatico:

a) utilizzo di supporti di memoria non personali ma di altri operatori;
b) uso di software gratuito o shareware scaricato da siti Internet o in allegato a riviste o libri;
c) uso di supporti di memoria preformattati;
d) collegamento in rete, nel quale il client avvia solo applicazioni residenti nel proprio disco rigido;
e) collegamento in rete, nel quale il client avvia anche applicazioni residenti sul disco rigido del server;
f) uso di modem per la posta elettronica e prelievo di file da BBS o da servizi commerciali in linea o da banche dati;
g) uso di modem mentre si è connessi alla rete intranet aziendale protetta;
h) ricezione di applicazioni e dati dall'esterno (Amministrazioni, fornitori, ecc.);
i) utilizzo dello stesso computer da parte di più persone;
j) collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
k) collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
l) file attached di posta elettronica.

Comportamenti che riducono il rischio di contrarre un virus informatico:

a) utilizzare soltanto programmi provenienti da fonti fidate.
   Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato ed autorizzato. Non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus;
b) assicurarsi che il proprio software antivirus sia aggiornato.
   La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus;
c) non diffondere messaggi di provenienza dubbia.
   Se si ricevono messaggi che avvisano di un nuovo virus pericolosissimo, è necessario ignorarli: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete;
d) non partecipare a "catene di S. Antonio" e simili.
   Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso;
e) limitare la trasmissione di file eseguibili (.com, .exe, .ovl, .ovr) e di sistema (.sys) tra computer in rete;
f) non utilizzare i server di rete come stazioni di lavoro;
g) non aggiungere mai dati o file a dispositivi contenenti programmi originali;
h) non condividere nessuna cartella del proprio computer ma utilizzare i file server o server ftp.

7. PROGRAMMI PER ELABORATORE VOLTI A PREVENIRE LA VULNERABILITÀ DEGLI STRUMENTI ELETTRONICI E A CORREGGERNE DIFETTI

1. sono adottati programmi che effettuano un aggiornamento costante dei prodotti, sistema operativo e applicazioni, non appena viene scoperto un bug, mediante installazione di patch che effettuano una verifica periodica dell'installazione e della configurazione dei prodotti software. L'aggiornamento periodico ha frequenza **almeno annuale** e, nel caso di trattamento di dati sensibili e giudiziari, **almeno semestrale**;
2. è adottato un sistema idoneo alla **registrazione degli accessi logici** (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica dell'attività dell'amministratore di sistema. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha

generate e devono essere conservate per un congruo periodo, **non inferiore a sei mesi**.

8. ISTRUZIONI ORGANIZZATIVE E TECNICHE PER IL SALVATAGGIO DEI DATI CON FREQUENZA ALMENO SETTIMANALE

L'integrità dei **dati sul server** è garantita da una doppia procedura di back-up:

1. la prima avviene in automatico con apposito software che giornalmente opera il salvataggio di una copia dei dati sul server stesso;
2. la seconda è effettuata copiando su supporto rimovibile (CD-ROM), con cadenza settimanale, i back-up di tutta la settimana eseguiti sul server.

I supporti rimovibili (CD-ROM) vengono conservati nell'armadio blindato dell'ufficio del DSGA. Lo stesso contiene anche le copie di salvataggio degli applicativi.

A livello locale di **personal computer (client)** la procedura di back-up avviene:

1. mediante il software antivirus installato che opera il salvataggio automatico di una copia dei dati impostato settimanalmente;
2. copiando su supporto rimovibile (chiave USB) i dati, sempre con cadenza settimanale.

I supporti rimovibili sono custoditi nell'armadio blindato dell'ufficio del DSGA.

I supporti rimovibili contenenti **dati sensibili e giudiziari** se non utilizzati vengono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, solo dopo aver reso le informazioni in essi contenuti non intelligibili e tecnicamente in alcun modo ricostruibili.

9. ISTRUZIONI TECNICHE E ORGANIZZATIVE PER LA CUSTODIA E L'USO DEI SUPPORTI RIMOVIBILI

Al fine di evitare accessi non autorizzati e trattamenti non consentiti, i supporti rimovibili (CD-ROM e chiavi USB) su cui sono memorizzati i dati, sono:

1. custoditi nell'armadio blindato dell'ufficio del DSGA al termine della giornata lavorativa;
2. conservati in cassetti chiusi a chiave durante il loro utilizzo. Inoltre devono essere eseguite le disposizioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, di cui al punto 7 delle Misure tecniche e organizzative - Trattamenti con strumenti elettronici;
3. formattati quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi. Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

10. MISURE PER GARANTIRE IL RIPRISTINO DELL'ACCESSO AI DATI IN CASO DI DANNEGGIAMENTO DEGLI STESSI O DEGLI STRUMENTI ELETTRONICI

1. La procedura di salvataggio periodico avviene mediante il software di back-up del programma di gestione amministrativa il quale crea in automatico, con cadenza giornaliera, una copia compressa dei dati, archiviandoli in un'apposita cartella del server, e di un masterizzatore *DVD* che salva i back-up di tutta la settimana su disco *DVD* registrabile, da utilizzare al termine della giornata lavorativa del venerdì.
2. Al termine della settimana lavorativa i singoli incaricati provvederanno ad effettuare il salvataggio dei dati su chiave *USB*. I supporti rimovibili sono custoditi all'interno dell'armadio blindato dell'ufficio del DSGA.
3. Il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento avverrà mediante l'utilizzo degli appositi back-up operati dai singoli incaricati.
   NOTE:
   a) *Il server è collegato ad un gruppo di continuità statico UPS che entra in funzione in seguito alla mancanza di corrente elettrica o a causa di sbalzi di tensione.*
   b) *I computer, incluso il server, sono sollevati da terra in modo da evitare eventuali perdite di dati dovuti ad allagamenti.*

11. MISURE DI SICUREZZA ESEGUITE DA SOGGETTI ESTERNI ALLA STRUTTURA

I soggetti esterni all'istituto scolastico (Amministratore di sistema, installatori, società di software e hardware, ecc.) che eseguono, per conto del titolare del trattamento, le misure minime di sicurezza riportate nei punti precedenti, devono presentare una **descrizione scritta dell'intervento effettuato** che ne attesti la conformità alle disposizioni di sicurezza adottate dall'istituto scolastico.