

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

IIS Severi-Correnti

Regolamento per l'esercizio del sistema di videosorveglianza dell'IIS Severi-Correnti, aggiornato al Reg. UE 2017/679 – GDPR, al D. Lgs. 196/2003 come modificato dal D. Lgs.101/2018 e al provvedimento 3/2019 dello European Data Protection Board sul trattamento dei dati personali attraverso dispositivi di videosorveglianza

Delibera n. 16 del consiglio d'istituto del 27 aprile 2021



Titolo documento: Regolamento per l'esercizio del sistema di videosorveglianza dell'IIS Severi-Correnti

Codice documento: IIS_Severi-Correnti – NUOVOREGVDS-1-0

Nome file: IIS_Severi-Correnti – NUOVOREGVDS Ver 1-0

Stato documento: Prima emissione ufficiale

Versione: 1.0

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
 Tel. 02 31 81 121 - Fax 02 89 05 52 63
 E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
 20121 Milano
 Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Data ultimo 12 gennaio 2021
aggiornamento

Indice

Art. 1 - Definizioni.....	4
Art. 2 - Obiettivo del presente Regolamento	7
Art. 3 - Ambito di validità e di applicazione del presente regolamento	8
Art. 4 - Identificazione del titolare del trattamento dei dati.....	9
Art. 5 - Obiettivi e finalità del sistema di videosorveglianza	10
Art. 6 – Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza e proporzionalità, e finalità.....	11
6.1 Premessa	11
6.2 Principio di liceità.....	11
6.3 Principio di necessità	12
6.4 Principio di non eccedenza e proporzionalità	13
6.5 Principio di finalità	14
Art. 7 – Utilizzi esplicitamente vietati	16
Art. 8 – Tipi di trattamenti autorizzati	17
Art. 9 – Tipologie di soggetti e di strutture coinvolte nelle operazioni di trattamento dei dati.....	19
Art. 10 – Accesso ai dati da parte delle Forze dell’Ordine e dell’Autorità Giudiziaria	20
Art. 11 – Accesso telematico da parte di soggetti incaricati di operazioni di assistenza e manutenzione	21
Art. 12 – Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento	23
Art. 13 – Designazione dei “soggetti autorizzati” ai sensi dell’art. 29 del GDPR	24
Art. 14 – Obblighi degli incaricati	25
Art. 15 – Orari di funzionamento del sistema di videosorveglianza	26
Art. 16 – Tempi di conservazione delle immagini.....	27
Art. 17 – Luogo e modalità di memorizzazione delle immagini	28
Art. 18 – Criteri e modalità di estrazione delle immagini	29
Art. 19 – Cifratura dei dati trasmessi mediante apparati e tecnologie wireless.....	30

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
 Tel. 02 31 81 121 - Fax 02 89 05 52 63
 E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
 20121 Milano
 Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 20 – Ottemperanza al Provvedimento del 27-11-2008 del Garante per la protezione dei dati personali relativo al controllo dell’operato degli amministratori di sistema.	31
Art. 21 – Installazione di nuove telecamere	33
26.2 - Tempi di conservazione delle immagini.....	34
26.3 - Utilizzi esplicitamente vietati	34
Art. 22 – Informativa	35
Art. 23 – Riscontro all’interessato	35
Art. 24 – Requisiti minimi sul luogo di collocazione del server	36
Art. 25 – Valutazione d’Impatto sulla Protezione dei Dati.....	37
Art. 26 - Effettuazione periodica di scansioni di vulnerabilità sulle piattaforme in cloud.....	37
Art. 27 - Notificazione al Garante per la protezione dei dati personali degli eventi di tipo “Violazione dei dati personali”	38
Art. 28 - Registro delle violazioni dei dati.....	38
Art. 29 – Requisiti minimi sugli strumenti elettronici, informatici e telematici.....	40
Art. 30 – Notificazione del trattamento al Garante per la protezione dei dati personali	42
Art. 31 – Cessazione del trattamento	43
Art. 32 – Danni cagionati per effetto del trattamento dei dati personali	43
Art. 33 – Comunicazione	43
Art. 34 – Modifiche e integrazioni regolamentari	44

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 1 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del Reg. UE 2016/679 – GDPR (per brevità nel seguito detto anche semplicemente “*Regolamento*” o “*GDPR*”).

Ai sensi dell'art. 4 del Regolamento si intende per:

- 1) «dati personali»: qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica;
- 2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- 4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «autorità competente»:

a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o

b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;

8) «titolare del trattamento»: l'autorità competente che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o dello Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione o dello Stato membro;

9) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

- 10) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o dello Stato membro non sono considerate destinatari; il trattamento di tali dati da parte di tali autorità pubbliche è conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento;
- 11) «violazione dei dati personali»: la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- 12) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- 13) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- 14) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- 15) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 41;
- 16) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 2 - Obiettivo del presente Regolamento

Obiettivo del presente regolamento è assicurare che i trattamenti di dati personali effettuati dall'IIS Severi-Correnti (nel seguito per brevità denominato anche **Istituto**) mediante il sistema di videosorveglianza, avvengano correttamente, lecitamente, e conformemente a quanto previsto dalla disciplina rilevante in materia di sicurezza e protezione dei dati personali; in particolare, il rispetto del presente regolamento garantirà la conformità:

- al Regolamento UE 2016/679 - GDPR
- alle prescrizioni del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali), così come modificato dal D.Lgs. 101/2018;
- ai provvedimenti del Garante per la protezione dei dati personali, con particolare riferimento al provvedimento generale del 8 aprile 2010 del Garante per la protezione dei dati personali, dedicato alla videosorveglianza;
- al provvedimento 3/2019 dello European Data Protection Board sul trattamento dei dati personali attraverso dispositivi di videosorveglianza;
- ai principi di:
 - liceità;
 - necessità;
 - finalità;
 - non eccedenza e proporzionalità rispetto alle finalità;
 - minimizzazione dei dati.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 3 - Ambito di validità e di applicazione del presente regolamento

Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali e sensibili effettuati mediante sistema di videosorveglianza:

- sotto la **diretta titolarità** dell'IIS Severi-Correnti, e
- all'interno delle aree di proprietà o di pertinenza dell'IIS Severi-Correnti.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 4 - Identificazione del titolare del trattamento dei dati

Il titolare dei trattamenti di dati personali effettuati mediante il sistema di videosorveglianza dell'IIS Severi-Correnti è l'IIS Severi-Correnti stesso: pertanto, competono esclusivamente all'Istituto le decisioni in ordine alle finalità e alle modalità del trattamento, compreso anche il profilo della sicurezza. A titolo esemplificativo e non esaustivo, si riportano di seguito alcune decisioni che spettano esclusivamente all'IIS Severi-Correnti:

- il numero, la tipologia e i luoghi di installazione attuale e futura delle telecamere;
- i tempi massimi e minimi di memorizzazione delle immagini;
- gli strumenti elettronici, informatici e telematici da utilizzare per la gestione delle immagini, compresa la ripresa e la memorizzazione delle immagini stesse;
- l'individuazione dei soggetti che possono essere a vario titolo coinvolti (in qualità di incaricati, oppure di responsabili interni od esterni oppure di autonomi titolari) nelle operazioni di trattamento dai dati e nelle operazioni di amministrazione di gestione di sistema informatico e telematico;
- l'individuazione di compiti e responsabilità da assegnare ai soggetti individuati in precedenza.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 5 - Obiettivi e finalità del sistema di videosorveglianza

Il sistema di videosorveglianza, in quanto sistema che comporta il trattamento di dati personali, può essere utilizzato esclusivamente per il perseguimento delle funzioni istituzionali del titolare del trattamento dei dati, vale a dire dell'IIS Severi-Correnti.

In via esemplificativa e non esaustiva le finalità sono:

- tutela del patrimonio dell'Istituto, di beni e di persone;
- prevenzione e rilevazione di reati;
- prevenzione e rilevazione di atti vandalici;
- raccolta e costituzione di materiale probatorio di natura fotografica e filmica a supporto delle attività di documentazione e comunicazione di notizie di reato;
- raccolta e costituzione di materiale probatorio di natura fotografica e filmica a supporto delle attività di accertamento, contestazione e notificazione di reati, ai sensi degli artt. 13 e 14 della Legge 24 novembre 1981, n. 689;
- supporto allo svolgimento di attività ed indagini di Polizia Giudiziaria da parte degli organi competenti;
- rilevazione di situazioni di pericolo l'utenza.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 6 – Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza e proporzionalità, e finalità.

6.1 Premessa

La verifica del rispetto dei principi di liceità, necessità, non eccedenza e proporzionalità e finalità dovrà venire effettuata periodicamente sia nei confronti del sistema di videosorveglianza nel suo complesso, sia nei confronti di ciascuna telecamera installata.

6.2 Principio di liceità

Affinché sia soddisfatto il principio di liceità, si dovrà periodicamente verificare che:

- le finalità perseguite mediante il sistema di videosorveglianza siano coerenti e compatibili con le funzioni istituzionali di competenza dell'IIS Severi-Correnti;
- la videosorveglianza non avvenga in violazione delle vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata (es. art. 615bis del Codice Penale), di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela;
- la videosorveglianza non abbia luogo in violazione delle tutele riconosciute ai lavoratori, con particolare riferimento a quanto previsto dalla Legge 300/1970 (Statuto dei Lavoratori);
- le riprese o le registrazioni non vengano effettuate in violazione di quanto previsto da disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi;

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

- la videosorveglianza avvenga nel rispetto delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni;
- siano osservati specifici limiti derivanti da disposizioni di legge o di regolamento che prevedono o ipotizzano la possibilità di installare apparecchiature di ripresa locale, aerea o satellitare (d.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, dalla legge 24 aprile 2003, n. 88), disposizioni che, quando sono trattati dati relativi a persone identificate o identificabili, vanno applicate nel rispetto dei principi affermati dal Codice, in tema per esempio di sicurezza presso stadi e impianti sportivi.

6.3 Principio di necessità

Affinché sia rispettato il principio di necessità deve essere escluso qualsiasi utilizzo superfluo ed evitati eccessi e ridondanze. Inoltre il sistema informatico e ciascuna telecamera deve essere configurata ed utilizzata in maniera tale da non utilizzare dati relativi a soggetti identificabili quando le finalità del trattamento possono essere perseguite raccogliendo solamente dati anonimi; inoltre il software deve essere configurato in modo da cancellare automaticamente e periodicamente i dati eventualmente registrati.

Ulteriori considerazioni da tenere presenti per il rispetto del principio di necessità sono le seguenti:

- l'esigenza di perseguire le finalità deve essere concreta, reale e comprovabile;
- il personale dipendente dell'Istituto, non potendo sempre essere presente e, non è in grado di assicurare il monitoraggio e la registrazione continua dei fatti, che solo un sistema di videosorveglianza può assicurare;
- da un punto di vista economico, l'utilizzo di un sistema elettronico di videosorveglianza presenta dei costi sensibilmente inferiori rispetto ai costi

<p>IIS Severi-Correnti</p> <p>Via Alcuino, 4 - 20149 Milano (MI) Tel. 02 31 81 121 - Fax 02 89 05 52 63 E-mail miis07200d@istruzione.it - PEC miis07200d@pec.istruzione.it</p>	<p>Capital Security Srls Via Montenapoleone, 8 20121 Milano Tel. 02-94750.267 info@capitalsecurity.it www.capitalsecurity.it</p>
--	---

derivanti dall'utilizzo di personale dedicato al perseguimento delle finalità indicate in precedenza;

- il sistema di videosorveglianza deve essere configurato per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

6.4 Principio di non eccedenza e proporzionalità

Il rispetto dei principi di non eccedenza e proporzionalità si dovrà valutare periodicamente con riferimento ai criteri di seguito elencati:

- il numero e la collocazione delle telecamere devono essere effettivamente commisurate al reale livello di rischio, evitando la rilevazione o la registrazione in aree che non siano soggette a concreti pericoli o che non siano meritevoli di particolare tutela;
- il posizionamento, la tipologia di telecamere, le aree brandeggiabili, l'utilizzo di zoom, quali dati ed eventi rilevare, devono essere rapportati alle concrete finalità ed esigenze, e si dovranno evitare eccedenze; ad esempio si dovrà limitare la possibilità di brandeggio mediante l'impostazione di vincoli o di mascheramenti statici;
- le telecamere devono essere collocate, e più in generale la videosorveglianza deve essere adottata, solo quando altre misure meno "invasive" siano state ponderatamente valutate insufficienti o inattuabili;
- se l'installazione delle telecamere è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri accorgimenti quali ad esempio controlli da parte di addetti,

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

sistemi di allarme, misure di protezione perimetrale e degli ingressi, abilitazione e controllo degli accessi;

- non è consentita l'installazione meramente dimostrativa o artefatta di telecamere non funzionanti o per finzione, che può essere legittimamente oggetto di contestazione;
- la non eccedenza e proporzionalità deve essere valutata, anche periodicamente, in ogni fase e modalità del trattamento; ad esempio, in fase di definizione e assegnazione dei profili di accesso ai dati, i profili dovranno essere configurati e assegnati in maniera che gli incaricati accedano alla minima quantità di dati necessaria per lo svolgimento dei compiti assegnati; come minimo si dovrà prevedere una fondamentale distinzione tra il profilo di tipo "utente normale" e un profilo più elevato di tipo "administrator";

6.5 Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi, ai sensi dell'art. 5 del GDPR; sono pertanto esclusi utilizzi indeterminati, occulti e non legittimi. In particolare il titolare o il responsabile potranno perseguire solo finalità di propria pertinenza.

Potranno essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività di Polizia Giudiziaria). E non finalità generiche o indeterminate, soprattutto quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti.

E' inoltre consentita la videosorveglianza come misura complementare volta a supportare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

difesa del titolare del trattamento o di terzi sulla base di immagini o riprese, in caso di atti illeciti.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 7 – Utilizzi esplicitamente vietati

Nel caso si presenti l'esigenza chiaramente dimostrabile e giustificabile, di effettuare riprese in luoghi chiusi pubblici o aperti al pubblico, si dovrà verificare e assicurare che le riprese avvengano nel pieno rispetto dello "Statuto dei lavoratori" e non violino il divieto, da parte del datore di lavoro, di effettuare controlli a distanza sull'attività dei dipendenti.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 8 – Tipi di trattamenti autorizzati

Nell'installazione e nell'esercizio del sistema di videosorveglianza, sono autorizzati esclusivamente le seguenti tipologie di trattamenti:

- installazione e attivazione di nuove telecamere;
- creazione e gestione di gruppi e profili di utenti;
- consultazione immagini live da telecamera;
- messa a fuoco e brandeggiamento della telecamera;
- impostazione di limiti al brandeggiamento delle telecamere
- impostazione di zone oscurate staticamente
- registrazione di immagini;
- cancellazione di immagini;
- predisposizione delle soglie temporali e degli eventi di cancellazione immagini;
- consultazione immagini registrate;
- estrazione (duplicazione) immagini registrate;
- definizione aree di motion-detection;
- definizione azioni da eseguire in concomitanza di eventi di motion-detection;
- accensione di sorgenti luminose o ad infrarosso;
- attivazione funzionalità di "speak-ip";
- rilevazione e inventario degli indirizzi ip presenti in rete;
- rilevazione e inventario dei mac address presenti in rete;
- installazione e configurazione di software applicativo;

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

- installazione e configurazione di software di base;
- installazione di “patch” e “hot fix”;
- attivazione collegamenti da remoto;
- interventi generici di manutenzione e configurazione hardware e software;
- estrazione di files di log;
- conservazione di files di log per un periodo minimo di dodici mesi;
- apposizione di firma digitale qualificata o di codici hash a files di log.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
 Tel. 02 31 81 121 - Fax 02 89 05 52 63
 E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
 20121 Milano
 Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 9 – Tipologie di soggetti e di strutture coinvolte nelle operazioni di trattamento dei dati

Le operazioni di trattamento dei dati saranno svolte – a vario titolo – dalle seguenti tipologie di soggetti:

- Titolare del trattamento dei dati;
- Responsabile della protezione dei dati, ai sensi degli artt. 37, 38 e 39 del GDPR;
- Responsabile esterno del trattamento dei dati: sono i soggetti (persone fisiche o giuridiche) esterni all'IIS Severi-Correnti ai quali sono affidati, da parte dell'IIS Severi-Correnti, alcune operazioni di trattamento dei dati e la messa in atto di alcune misure di sicurezza;
- Incaricati del trattamento dei dati: sono i soggetti fisici (persone fisiche) che, designati per iscritto dal titolare o dal responsabile, eseguono una o più operazioni di trattamento dei dati;
- Custode delle password di sistema: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell'amministratore di sistema - delle parole chiave corrispondenti ai vari profili di tipo "administrator" o equivalenti;
- Custode delle parole chiave: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell'incaricato – delle parole chiave assegnate agli utenti finali;
- Soggetti incaricati della gestione e manutenzione degli strumenti elettronici, denominati anche "Amministratori di sistema";

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 10 – Accesso ai dati da parte delle Forze dell’Ordine e dell’Autorità Giudiziaria

Il D. Lgs. 196/2003, così come modificato dal D. Lgs. 101/2018, prevede che la comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico possa avvenire se:

- prevista da norma di legge o di regolamento, oppure
- anche in assenza di norma di legge o di regolamento, sia necessaria per lo svolgimento delle funzioni istituzionali.

Pertanto le Forze dell’Ordine o l’Autorità Giudiziaria possono lecitamente richiedere di:

- accedere alle immagini “live”;
- accedere alle immagini registrate ed ottenute copia delle registrazioni;
- effettuare riprese e registrazioni “ad-hoc”.

La mancata o tardiva concessione dell’accesso potrà comportare, a carico del soggetto responsabile, il reato di omissione di atti d’ufficio e di ostacolo alle indagini.

Le richieste di accesso/estrazioni dovranno seguire le procedure definite nel presente regolamento, ed essere autorizzate per iscritto dal Dirigente Scolastico.

In ogni caso, l’utilizzo delle immagini da parte di qualsiasi soggetto pubblico che per l’esercizio delle proprie funzioni istituzionali abbia necessità di accedere ai dati, dovrà avvenire conformemente a quanto previsto dall’art. 5 del GDPR e più in generale dalla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento al provvedimento generale del Garante per la protezione dei dati personali del 8 aprile 2010, dedicato alla videosorveglianza.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 11 – Accesso telematico da parte di soggetti incaricati di operazioni di assistenza e manutenzione

E' previsto che per l'effettuazione di alcune operazioni di assistenza e manutenzione da parte di soggetti opportunamente designati in qualità di responsabili esterni del trattamento dei dati ai sensi dell'art. 28 del GDPR, possa avere luogo in modalità "telemantenzione", laddove tale prassi sia esplicitamente prevista dai contratti di assistenza.

In ogni caso la gestione della telemantenzione dovrà soddisfare come minimo i seguenti requisiti di base:

- monitoraggio effettuato tramite protocollo SNMP – Simple Network Management Protocol, o equivalente, che in caso di problemi invia un'e-mail alla ditta incaricata della telemantenzione che viene letta in orario lavorativo, di tutti gli apparati costituenti il sistema di Videosorveglianza:

- telecamere digitali o analogiche
- apparati trasmissivi di rete d'accesso di tipo CPE;
- apparati trasmissivi di dorsale di tipo AP – Access Point;
- apparati trasmissivi di backbone di tipo PTP – Point To Point;
- switch;
- router;
- server e client;
- NAS e apparati di memorizzazione dei dati;
- raid controller;

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

- impiego dell'ampiezza di banda;
- nomi dei dispositivi monitorati;
- accesso remoto e locale limitato alla sola rete del sistema di videosorveglianza: non dovrà essere possibile in nessun modo accedere a reti o sottoreti diverse da quelle usate per il sistema di videosorveglianza;
- accesso remoto effettuato esclusivamente su tratte cifrate, ad esempio mediante VPN;
- identificazione certa dei soggetti che accedono da remoto;
- tracciatura degli accessi e delle operazioni effettuate;
- accesso al sistema di videosorveglianza negoziato ed autorizzato di volta in volta da personale designato per iscritto dell'IIS Severi-Correnti.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 12 – Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento

In generale i soggetti coinvolti nelle operazioni di trattamento dovranno essere designati per iscritto dal titolare o dal responsabile del trattamento dei dati, con atto che specifichi chiaramente compiti e responsabilità assegnate. Per quanto riguarda gli incaricati del trattamento dei dati, detti anche “soggetti designati” ai sensi dell’art. 29 del GDPR, oltre ai compiti e alle responsabilità affidate, dovrà essere chiaramente specificato l’ambito del trattamento consentito.

La revisione della sussistenza delle condizioni per il mantenimento dell’ambito del trattamento consentito e del profilo di accesso dovranno essere oggetto di revisione da parte del responsabile o del titolare con frequenza almeno annuale.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 13 – Designazione dei “soggetti autorizzati” ai sensi dell’art. 29 del GDPR

Coerentemente con quanto prescritto dal punto 3.3.2. del Provvedimento del Garante per la protezione dei dati personali del 8 aprile 2010, la designazione degli incaricati dovrà avvenire con modalità che permettano di esplicitare con la massima granularità le tipologie di operazioni alle quali ciascun incaricato risulterà essere abilitato. L’ambito del trattamento consentito agli incaricati dovrà inoltre essere oggetto di verifica (ed eventuale modifica) almeno annuale.

La designazione dei soggetti incaricati ed autorizzati dovrà essere effettuata ai sensi dell’art. 29 del GDPR.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 14 – Obblighi degli incaricati

Fatti salvi i casi di richiesta degli interessati, i dati registrati possono essere riesaminati, nel limite di tempo ammesso dal presente regolamento, solo in caso di effettiva necessità e per l'esclusivo perseguimento delle finalità di cui all'art. 5. In ogni caso, l'estrazione di immagini potrà avvenire solo in caso di richiesta/autorizzazione scritta da parte del Dirigente Scolastico, oppure di richiesta proveniente da altra Pubblica Amministrazione, nei casi in cui l'accesso a immagini registrate sia necessario per lo svolgimento delle funzioni istituzionali. Anche in questo ultimo caso l'accesso/estrazione delle immagini dovrà essere autorizzata dal Dirigente Scolastico

La mancata osservanza degli obblighi di cui al presente articolo potrà comportare l'applicazione di sanzioni disciplinari ed amministrative, e, ove previsto dalla vigente normativa, l'avvio di procedimenti penali.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 15 – Orari di funzionamento del sistema di videosorveglianza

Il sistema di videosorveglianza potrà registrare le immagini solo durante l'orario di chiusura dell'Istituto, nel caso di telecamere installate all'interno dei locali dell'Istituto stesso. Una deroga è costituita dalle telecamere utilizzate per controllare gli accessi (es. entrate di servizio), nel qual caso potranno essere sempre attive.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 16 – Tempi di conservazione delle immagini

I tempi di conservazione dei dati gestiti mediante il sistema di videosorveglianza dovranno tenere conto della tipologia di dati, delle finalità per le quali i dati sono acquisiti e trattati, nonché di eventuali prescrizioni/limiti imposti dalla attuale normativa in materia di videosorveglianza e protezione dei dati personali.

Per quanto riguarda le immagini acquisite mediante le telecamere convenzionali (non di tipo per la rilevazione delle targhe dei veicoli in transito), in considerazione delle finalità individuate in precedenza, e della necessità di ottemperare al principio di non eccedenza e proporzionalità in tutte le operazioni di trattamento dei dati, le immagini registrate dovranno essere conservate per un tempo massimo di **7 giorni**; dovrà comunque essere presente una funzionalità che permetta agevolmente di disattivare la cancellazione automatica – trascorso il tempo massimo di registrazione - delle immagini registrate (ad esempio in concomitanza della registrazione di atti vandalici), senza impedire o menomare la capacità di registrare le immagini “in diretta”. E' inoltre prevista la possibilità che i tempi di memorizzazione delle immagini possano venire modificati a seguito di variazioni nelle finalità, di mutate esigenze, oppure di motivata richiesta proveniente dalle Forze dell'Ordine.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 17 – Luogo e modalità di memorizzazione delle immagini

Le immagini riprese dalle telecamere dovranno essere memorizzate in formato elettronico su un unico (o un numero limitato) supporto di memorizzazione di massa centralizzato e ben individuato all'interno di un unico e ben determinato apparato di tipo "server" (può essere comunque fatta salva la necessità di una memorizzazione "di backup" su un server remoto). Il suddetto server dovrà essere dedicato esclusivamente alla memorizzazione delle immagini registrate dalle telecamere del sistema di videosorveglianza, e non dovrà essere dedicato ad altri scopi. Se non diversamente disposto dal titolare con atto scritto, il server non dovrà essere collegato ad internet, oppure dovrà essere collegato solo in casi e per finalità specifiche e ben individuate, per intervalli di tempo il più possibile contenuti.

Una eventuale deroga al punto precedente è permessa nel caso il sistema di videosorveglianza si basi su una architettura in cloud, nel qual caso le immagini possono essere memorizzate su un server remoto raggiungibile tramite internet, ed eventualmente su un server locale.

Non è consentita la memorizzazione "ordinaria" delle immagini in locale a livello di postazione "client", o comunque su supporti e strumenti diversi dal succitato server centralizzato. La memorizzazione temporanea delle immagini in locale potrà avvenire solo in caso di estrazione di immagini, nel qual caso la copia temporanea locale delle immagini estratte dovrà essere cancellata non appena possibile.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 18 – Criteri e modalità di estrazione delle immagini

L'estrazione delle immagini dovrà avvenire in conformità a quanto specificato nei seguenti passi operativi:

- viene ricevuta la richiesta di estrazione;
- il Dirigente Scolastico autorizza o meno l'estrazione delle riprese filmiche. Nel caso l'estrazione sia autorizzata:
 - o l'incaricato individuato provvede ad effettuare l'estrazione delle riprese filmiche
 - o vengono predisposte due copie delle sequenze filmiche estratte, di cui una rimane agli atti
 - o si effettua la consegna con contestuale redazione del verbale di consegna o nota che dovrà essere successivamente archiviato.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 19 – Cifratura dei dati trasmessi mediante appareti e tecnologie wireless

I dati trasmessi mediante apparecchi wireless dovranno essere cifrati, in maniera che ne sia garantita la riservatezza. Come minimo dovranno essere applicati algoritmi di cifratura dotati di robustezza maggiore o uguale a DES (Data Encryption Standard).

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 20 – Ottemperanza al Provvedimento del 27-11-2008 del Garante per la protezione dei dati personali relativo al controllo dell’operato degli amministratori di sistema.

Per garantire l’ottemperanza a quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 27-11-2008 relativo al controllo dell’operato degli amministratori di sistema, il presente Regolamento prevede quanto segue:

- a livello di software di videosorveglianza, deve essere attivato (ed eventualmente configurato) un meccanismo di logging (tracciatura) delle operazioni di amministrazione e gestione di sistema effettuate con profilo di administrator;
- a livello di software di videosorveglianza, il suddetto file di log non deve essere sovrascritto per un periodo minimo di tre mesi;
- il suddetto file di log non dovrà essere per nessun motivo cancellato, modificato o alterato;
- con frequenza al massimo semestrale, si dovrà procedere all’estrazione (copia) del suddetto file di log;
- la copia estratta del file di log dovrà essere generata in un formato non modificabile (pdf, tiff o altri formati non modificabili) e firmata digitalmente con certificato digitale emesso da una certification authority trusted di primo livello;
- la copia del file di log firmata digitalmente dovrà essere custodita in un luogo sicuro per un periodo di almeno 12 mesi;
- con frequenza almeno semestrale si dovrà controllare l’operato degli amministratori di sistema, mediante analisi dei file di log e del registro

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

delle operazioni di amministrazione e gestione di sistema effettuate sul sistema di videosorveglianza; alla conclusione delle operazioni di controllo / verifica dovrà essere redatto apposito verbale e relazione.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 21 – Installazione di nuove telecamere

L'installazione di nuove telecamere dovrà essere autorizzata dal Consiglio di Istituto. Preventivamente si dovrà verificare che:

- i luoghi ripresi;
- le telecamere utilizzate;
- le configurazione e la possibilità di utilizzo delle telecamere delle riprese e delle registrazioni effettuate;

soddisfino i principi di liceità, necessità, non eccedenza e proporzionalità e finalità.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

26.2 - Tempi di conservazione delle immagini

Le immagini registrate mediante le telecamere indossabili devono essere conservate per un periodo di sette giorni solari. Qualora non siano disponibili meccanismi automatici mediante i quali le immagini sono automaticamente cancellate trascorsi sette giorni solari dalla data di acquisizione, devono essere previsti meccanismi manuali di cancellazione delle immagini e delle riprese filmiche.

26.3 - Utilizzi esplicitamente vietati

Le immagini e le riprese filmiche non potranno essere utilizzate per effettuare attività di controllo a distanza del personale, ne' per valutare le prestazioni e le performance dei lavoratori; inoltre, le immagini e le riprese filmiche acquisite mediante telecamere indossabili non possono essere utilizzate per irrogare sanzioni disciplinari.

E' esplicitamente vietato qualsiasi tipo di diffusione delle immagini registrate, con particolare riferimento alla diffusione mediante pubblicazione su internet (es. pubblicazione su social network).

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 22 – Informativa

Gli utenti (dipendenti, alunni, genitori, fornitori etc.) devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata, e dell'eventuale registrazione, mediante un modello semplificato di informativa "minima" conforme a quanto previsto dal provvedimento 3/2019 dello European Data Protection Board sul trattamento dei dati personali attraverso dispositivi di videosorveglianza.

In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vanno installati più cartelli.

E' necessario controllare periodicamente che i cartelli siano presenti e ben leggibili, e non siano stati oggetto di atti vandalici o di eventi (es. crescita di rami o foglie, interposizione di altri elementi, etc.) che abbiano compromesso la piena leggibilità del testo e della rappresentazione iconica. In ogni caso, la leggibilità dovrà essere tempestivamente ripristinata e assicurata.

Art. 23 – Riscontro all'interessato

In caso di esercizio da parte degli interessati dei diritti previsti dagli artt. Da 15 a 22 del GDPR, il riscontro all'interessato dovrà essere fornito a cura del Titolare, **entro massimo 15 giorni lavorativi dalla data di ricezione della richiesta**. Le richieste di cancellazione o blocco dei dati dovranno essere soddisfatte esclusivamente nei casi in cui il trattamento sia avvenuto in violazione di legge, e comunque solo su autorizzazione scritta del Dirigente Scolastico. Non potranno essere oggetto di cancellazione o modifica le immagini per le quali vi siano state richieste di estrazione o siano in corso indagini da parte degli organi di Polizia o da parte dell'Autorità Giudiziaria.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 24 – Requisiti minimi sul luogo di collocazione del server

Il server di memorizzazione delle immagini dovrà essere fisicamente collocato all'interno di un locale che fornisca adeguate garanzie di sicurezza fisica e perimetrale. Di seguito si riportano i requisiti minimi che il locale dovrà soddisfare:

- locale ad utilizzo non promiscuo e dedicato esclusivamente a “sala macchine” o “sala server”, non agevolmente accessibile al pubblico e ai dipendenti (ad eccezione ovviamente dei dipendenti o collaboratori esplicitamente incaricati di operazioni di amministrazione e gestione di sistema);
- possibilità di regolamentare e di tenere traccia degli accessi al locale;
- locale di norma chiuso a chiave, con serratura e chiave funzionante;
- in caso vi siano finestre a piano terra, presenza di inferriate in ferro non dolce oppure presenza di vetri antisfondamento;
- assenza di carta, cartoni o altro materiale facilmente infiammabile all'interno del locale;
- presenza nelle vicinanze di almeno un estintore non a polvere, funzionante e regolarmente revisionato con frequenza almeno semestrale;
- presenza di adeguato impianto di condizionamento, che assicuri un livello di umidità e temperatura all'interno del range di corretto funzionamento degli apparati.

In aggiunta a quanto elencato, è auspicabile (ancorché non strettamente obbligatoria) la presenza di quanto segue:

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

- allarme volumetrico (attivato dalla variazione della volumetria all'interno dei locali) o di prossimità;
- presenza di sensori per la rilevazione del fumo e/o della temperatura;
- collegamento dei sensori e dell'allarme con centrale operativa di sicurezza oppure con le forze dell'ordine.

Art. 25 – Valutazione d’Impatto sulla Protezione dei Dati

Ai sensi dell’art. 23 del D. Lgs. 51/2019, il sistema di videosorveglianza potrà essere sottoposto a valutazione d’impatto sulla protezione dei dati laddove il trattamento presenti rischi significativi per i diritti e la libertà delle persone fisiche oggetto di trattamento.

La valutazione d’impatto dovrà contenere come minimo una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente regolamento.

Art. 26 - Effettuazione periodica di scansioni di vulnerabilità sulle piattaforme in cloud

Nel caso siano utilizzate piattaforme in cloud (ad esempio E-Surv), dovranno essere effettuate con frequenza mensile delle scansioni di vulnerabilità per individuare e documentare debolezze e configurazioni poco sicure, e per svolgere le attività di remediation.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Le scansioni di vulnerabilità verranno effettuate a cura del Responsabile della protezione dei dati con frequenza orientativamente mensile utilizzando piattaforme professionali di vulnerability assessment.

A fronte di richiesta da parte del Dirigente Scolastico, potranno venire effettuate su una-tantum delle scansioni di vulnerabilità su altri oggetti esposti direttamente su internet, come ad esempio firewall, router etc.

Art. 27 - Notificazione al Garante per la protezione dei dati personali degli eventi di tipo “Violazione dei dati personali”

Nel caso si verifichi un qualsiasi tipo di violazione dei dati, o se ne abbia anche solamente il sospetto, ne deve essere data immediata comunicazione al Dirigente Scolastico e al Responsabile della protezione dei dati, i quali quale si attiveranno immediatamente per valutare se vi sia stata effettivamente una violazione, la portata e le conseguenze, e valutare se sussistano i presupposti per effettuare la notificazione entro 72 ore all'autorità di controllo.

Art. 28 - Registro delle violazioni dei dati

Coerentemente con quanto previsto dall'art. 33 comma 5 del GDPR, deve essere in ogni caso tenuto un registro di tutte le violazioni di dati verificatesi, a prescindere dal fatto che siano state notificate all'autorità di controllo. Il suddetto registro deve contenere come minimo le seguenti informazioni:

- data della violazione

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

- descrizione delle circostanze e dell'evento
- tipologia e quantità di interessati impattati
- conseguenze della violazione
- data di comunicazione della violazione al Garante per la protezione dei dati (se la comunicazione è stata effettuata).

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 29 – Requisiti minimi sugli strumenti elettronici, informatici e telematici.

Gli strumenti elettronici, informatici e telematici utilizzati nelle operazioni di trattamento dei dati, dovranno soddisfare i seguenti requisiti minimi:

- sistema operativo server e client non obsoleto e con supporto attivo da parte del fornitore;
- server e client protetti da password iniziale di accesso al sistema operativo e alle risorse di rete; possibilità da parte dell'utente finale di modificare autonomamente la propria password; possibilità da parte dell'amministratore di sistema di disabilitare la user-id senza cancellarla;
- server e client protetti da password iniziale di accesso al programma applicativo; possibilità da parte dell'utente finale di modificare autonomamente la propria password; possibilità di disabilitare (da parte dell'amministratore di sistema) le user-id senza cancellarla;
- presenza di almeno due profili distinti: uno di tipo "administrator" e uno di tipo "utente normale", sia a livello di sistema operativo sia a livello di programma applicativo;
- assegnazione e utilizzo delle user-id su base strettamente personale e non di gruppo;
- possibilità di individuare e rimuovere periodicamente le vulnerabilità e le configurazioni poco sicure a livello applicativo e di sistema operativo;
- protezione adeguata da virus e codici maligni;
- protezione perimetrale adeguata in caso di apertura, anche temporanea, ad Internet.

I requisiti di cui sopra dovranno essere verificati con frequenza almeno semestrale mediante verifiche in loco dei locali, degli apparati e dei programmi, effettuando un'analisi dei rischi e individuando le azioni correttive da mettere in atto. Periodicamente si dovrà inoltre verificare che le

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

misure pianificate siano state messe in atto, e il livello di efficacia delle misure stesse. Di tutto quanto appena elencato si dovrà redigere apposita relazione da discutere con il Dirigente Scolastico.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 30 – Notificazione del trattamento al Garante per la protezione dei dati personali

Con l'entrata in vigore del D.Lgs. 101/2018, l'art. 37 del D.Lgs. 196/2003, che richiedeva per alcuni trattamenti l'obbligo di notifica del trattamento al Garante per la protezione dei dati personali, è stato abrogato.

Non è pertanto necessario effettuare alcuna notificazione al Garante per la protezione dei dati personali) dei trattamenti effettuati con il sistema di Videosorveglianza.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 31 – Cessazione del trattamento

In caso di cessazione del trattamento, i dati dovranno essere distrutti, ad eccezione di quelli per i quali siano in corso o vi siano state in passato richieste di estrazione, che dovranno essere conservati a cura del titolare per fini di documentazione e riscontro.

Art. 32 – Danni cagionati per effetto del trattamento dei dati personali

La materia è disciplinata dall'art. 82 del GDPR.

Art. 33 – Comunicazione

La comunicazione di dati personali da parte del titolare ad altri soggetti pubblici è ammessa quando è prevista da norma di legge o di regolamento attuativo di norma di legge, oppure quando risulti comunque necessaria per lo svolgimento delle funzioni istituzionali.

La comunicazione di dati personali da parte del titolare a privati o ad enti pubblici economici è ammessa unicamente quando prevista da norma di legge o di regolamento.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 34 – Modifiche e integrazioni regolamentari

Il presente regolamento dovrà essere adeguato per recepire eventuali modifiche alla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento alle disposizioni relative alla videosorveglianza.

Inoltre, il presente regolamento dovrà essere modificato nel caso dovessero mutare le finalità del sistema di videosorveglianza oppure introdotte significative novità di tipo tecnologico.

IIS Severi-Correnti

Via Alcuino, 4 - 20149 Milano (MI)
Tel. 02 31 81 121 - Fax 02 89 05 52 63
E-mail miis07200d@istruzione.it - PEC
miis07200d@pec.istruzione.it

Capital Security Srls

Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it