



POLITECNICO
MILANO 1863

POLITECNICO DI MILANO

IL DIRETTORE GENERALE

VISTA la Legge 20.05.970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento", e successive modifiche;

VISTO il D. Lgs. 30 marzo 2001, n. 165 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", e successive modifiche;

VISTO il D. Lgs. 30.06.2003, n. 196 recante "Codice in materia di protezione dei dati personali", e successive modifiche;

VISTO il 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 (regolamento generale sulla protezione dei dati);

VISTO il Provvedimento del Garante per la protezione dati in materia di videosorveglianza del 08.04.2010, e modifiche ed integrazioni a seguire;

VISTE le Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29.01.2020 dal Comitato Europeo per la Protezione dei Dati;

VISTO lo Statuto vigente del Politecnico di Milano;

VISTO il Regolamento Generale di Ateneo vigente;

VISTO il Codice etico e di comportamento del Politecnico di Milano vigente;

VISTO il Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT vigente e il conseguente Modello organizzativo privacy;

VISTO il Decreto del Direttore Generale n. 95745 del 21.04.2023 quale atto generale e organizzativo relativo alla sottoscrizione di atti e di documenti da parte dei soggetti statutari e amministrativi del Politecnico di Milano a ciò preposti,

VISTE le determinazioni del Direttore Generale in ordine all'articolazione delle Aree dirigenziali dell'Amministrazione del Politecnico di Milano, tra cui l'Area Gestione Infrastrutture e Servizi (nel seguito AGIS) che ha tra le competenze attribuite anche la gestione del Sistema di controllo accessi, allarme intrusione e supervisione fire&gas e del Sistema di videosorveglianza (TVCC);

RAVVISATA la necessità definire le regole e le modalità di gestione del sistema di videosorveglianza in capo all'Area Gestione Infrastrutture e Servizi del Politecnico di Milano mediante l'adozione di apposito disciplinare;

ADOTTA

- 1) Il Disciplinare per il Sistema di Videosorveglianza condotto dall'Area Gestione Infrastrutture e Servizi del Politecnico di Milano, il cui testo è allegato ed è parte integrante del presente atto amministrativo generale.
- 2) Eventuali modifiche ed integrazioni al Disciplinare sono disposte con decreti del Direttore Generale e sono immediatamente esecutive.
- 3) Con successivo decreto direttoriale saranno disposte le nomine del personale afferente all'Area Gestione Infrastrutture e Servizi cui sono attribuiti i compiti previsti nel paragrafo 2 "Organizzazione" del Disciplinare.

IL DIRETTORE GENERALE
Ing. Graziano Dragoni

Firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale e s.m.i.



POLITECNICO
MILANO 1863

**DISCIPLINARE PER IL SISTEMA DI VIDEOSORVEGLIANZA CONDOTTO DALL'AREA GESTIONE
INFRASTRUTTURE E SERVIZI DEL POLITECNICO DI MILANO**

INDICE

1.	PREMESSA.....	1
1.1	Scopo e campo di applicazione	1
1.2	Riferimenti normativi.....	1
1.3	Definizioni ed abbreviazioni	1
1.4	Descrizione del VSS.....	2
2.	ORGANIZZAZIONE	3
2.1	Ruoli, funzioni e responsabilità	3
2.1.1	Titolare del trattamento 5	
2.1.2	Responsabile interno del trattamento (Designato)	5
2.1.3	Responsabili esterni del trattamento.....	5
2.1.4	Autorizzati al trattamento	5
2.1.5	Amministratori di sistema.....	5
2.1.6	Responsabile della Protezione dei Dati.....	6
3.	DISPOSIZIONI.....	6
3.1	Principi generali del trattamento	6
3.2	Finalità del trattamento	7
3.3	Base giuridica del trattamento.....	7
3.4	Impatto del trattamento	7
3.5	Durata di conservazione delle registrazioni	7
3.6	Informativa trattamento dati personali	8
3.7	Esercizio dei diritti dell'interessato.....	8
4.	PROCESSI E PROCEDURE.....	8
4.1	Realizzazione, modifica e dismissione degli impianti di videosorveglianza.....	8
4.2	Accesso alle immagini in tempo reale.....	9
4.3	Trattamento delle immagini registrate.....	9
4.3.1	Consultazione visiva delle immagini registrate.....	9
4.3.2	Conservazione di copie delle immagini.....	9
4.3.3	Eliminazione delle copie delle immagini	10
4.3.4	Processo di produzione e comunicazione di copie delle immagini registrate.....	10
4.4	Registrazione degli accessi al VSS	12

1. PREMESSA

1.1 Scopo e campo di applicazione

Il presente Disciplinare descrive l'assetto organizzativo, le regole e le procedure operative per la conduzione del sistema di videosorveglianza (VSS, Video Surveillance System) installato con finalità di sicurezza dei beni e delle persone presso le sedi del Politecnico di Milano (Titolare del trattamento).

Il Disciplinare si applica esclusivamente al sistema degli impianti condotti, anche attraverso il supporto di ditte esterne, dall'Area Gestione Infrastrutture e Servizi del Politecnico di Milano (AGIS).

Sono esclusi dal campo di applicazione eventuali altri sistemi di videosorveglianza presenti in Ateneo e gestiti da soggetti terzi ad AGIS.

1.2 Riferimenti normativi

- **D.Lgs. 196/2003** "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018.
- **Provvedimento del Garante per la Protezione dei Dati Personali - 27 novembre 2008** "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i.
- **Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.** Regolamento Generale sulla Protezione dei Dati (General Data Protection Regulation o GDPR).
- **Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza - 8 aprile 2010.**
- **D.Lgs. 101/2018** "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 (regolamento generale sulla protezione dei dati)".
- **Linee guida EDPB 3/2019** sul trattamento dei dati personali attraverso dispositivi video emanate dal Comitato Europeo per la protezione dei dati (European Data Protection Board), versione 2.0 - 29 gennaio 2020.
- **Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT.**
- **Modello organizzativo Privacy ed istruzioni operative del Politecnico di Milano.**

1.3 Definizioni ed abbreviazioni

- **AGIS.** Area Gestione Infrastrutture e Servizi del Politecnico di Milano.
- **Amministratore di Sistema.** Soggetto incaricato della gestione e manutenzione di un impianto di elaborazione dati o delle sue componenti, ivi comprese le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi informatici complessi.
- **ASICT.** Area Servizi ICT del Politecnico di Milano.
- **Ateneo.** Il Politecnico di Milano.
- **Autorizzato al trattamento.** Persona fisica incaricata allo svolgimento delle operazioni di trattamento sui dati personali. L'Autorizzato opera in subordinazione al Titolare ed al suo diretto responsabile (Responsabile interno del trattamento o Responsabile esterno del trattamento).
- **Comunicazione.** Il dare conoscenza dei dati personali ad uno o più soggetti determinati, in qualunque forma, anche mediante la loro messa a disposizione per consultazione.
- **Control Room AGIS.** Struttura operativa centralizzata che svolge le funzioni di monitoraggio delle immagini di tutte le telecamere del sistema di videosorveglianza e dove vengono effettuate le operazioni di selezione ed estrazione delle immagini registrate.

- **Dato personale.** Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili anche indirettamente e rilevati con trattamenti delle immagini effettuati attraverso l'impianto di videosorveglianza.
- **DPIA (Data Protection Impact Assessment).** Processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità nonché a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
- **DPO (Data Protection Officer).** Responsabile della Protezione dei Dati, come definito dagli artt. 37-39 GDPR.
- **Garante.** Autorità Garante per la protezione dei dati personali.
- **GDPR (General Data Protection Regulation).** Regolamento UE 2016/679.
- **Interessato.** Persona fisica a cui si riferiscono i dati personali oggetto di trattamento in occasione dell'accesso all'area videosorvegliata (soggetto ripreso).
- **Responsabile esterno del trattamento.** Persona fisica o giuridica, autorità pubblica o altro organismo che tratta dati personali per conto del Titolare (ex art. 28 GDPR). Per i servizi svolti in outsourcing per conto del Titolare, è l'outsourcer che tratta dati personali.
- **Responsabile interno del trattamento (Designato).** Persona fisica espressamente designata dal Titolare, nell'ambito del proprio assetto organizzativo, a cui sono affidati gli adempimenti necessari e conseguenti all'attuazione delle norme in materia di protezione dei dati.
- **Terzo.** Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che non sia l'Interessato (soggetto ripreso), il Titolare del trattamento, il Responsabile del trattamento o i soggetti autorizzati al trattamento dei dati personali. A titolo esemplificativo, le Autorità o qualunque soggetto (denunciante o querelante) portatore di un interesse diretto concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata alle immagini alle quali è chiesto l'accesso.
- **Titolare del trattamento.** Organizzazione, in persona dell'organo di rappresentanza o soggetto da esso espressamente delegato, alla quale compete il potere decisionale autonomo in ordine alle finalità ed alle modalità del trattamento dei dati personali.
- **Trattamento.** Qualsiasi operazione o complesso 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.
- **Videosorveglianza.** Attività che comporta la raccolta e la conservazione di immagini ed informazioni grafiche delle persone che entrano nello spazio monitorato. La raccolta, la registrazione, la conservazione ed in generale l'utilizzo di immagini configura un trattamento di dati personali.
- **VMS (Video Management System).** Applicazione software per il monitoraggio ed il controllo dei componenti costituenti l'impianto di videosorveglianza.
- **VSS (Video Surveillance System).** Secondo la Norma CEI EN 62762-1-1 "Sistemi di videosorveglianza per applicazioni di sicurezza. Parte 1-1: Requisiti di sistema – Generalità", è un sistema composto da dispositivi di ripresa, di memorizzazione, di visualizzazione ed altri equipaggiamenti per la trasmissione dei dati ed il controllo.

1.4 Descrizione del VSS

Il VSS è composto da telecamere dislocate presso varie sedi dell'Ateneo volte ad inquadrare prevalentemente aree perimetrali esterne, in corrispondenza degli accessi al campus ed agli edifici, ed aree soggette a concrete esigenze di sicurezza (aree sensibili o pericolose).

Tutte le telecamere del VSS sono di tipo digitale, con orientamento fisso, attivate in registrazione 24/365 con modalità motion-detection. Risoluzione e frame-rate sono impostate per ottenere il rilevamento ed il riconoscimento dei soggetti ripresi.

La funzione di ripresa audio, ove la telecamera ne sia provvista, è disabilitata.

I dispositivi del VSS sono attestati su VLAN (Virtual Local Area Network), riservate al traffico dei sistemi di videosorveglianza, amministrate da ASICT.

L'applicazione VMS utilizzata per la gestione del sistema di videosorveglianza è CathexisVision di Cathexis.

Il sistema è costituito da 2 server di management (primario + failover) in ambiente virtualizzato.

L'archiviazione dei flussi video avviene (in modalità crittografata) su 2 apposite unità di storage di classe enterprise (primaria + failover) configurate in RAID (Redundant Array of Inexpensive Disks) di livello 5. Parallelamente, il VMS gestisce l'archiviazione periferica dei flussi video sulle schede di memoria a bordo delle telecamere (garantendo così la possibilità di recuperare, in maniera automatica, parti delle registrazioni in caso problemi di comunicazione della telecamera con il server VMS).

I server di management e le annesse unità di storage sono collocati in luoghi protetti ad accesso controllato, all'interno delle Server Farm di Ateneo.

I flussi video in tempo reale delle telecamere sono accessibili attraverso un numero dedicato di postazioni client collocate presso le principali portinerie di campus e presidiate da operatori autorizzati (ciascuna postazione consente la visione delle sole telecamere di propria competenza geografica). Una ulteriore postazione client, collocata nella Control Room tecnologica di Ateneo, supervisiona l'intero parco delle telecamere.

Per l'accesso alle immagini (in tempo reale e registrate) è necessario autenticarsi al sistema disponendo di un profilo personalizzato. Il sistema è impostato per registrare ogni accesso allo stesso.

La tecnologia utilizzata e le procedure di sicurezza applicate consentono la visione dei flussi video in tempo reale e la conservazione delle registrazioni in condizioni di sicurezza logica, fisica e ambientale, come richiesto dalla vigente normativa.

L'accesso remoto al VSS è effettuato esclusivamente per attività di manutenzione applicativa della piattaforma VMS ed avviene attraverso VPN (Virtual Private Network) nominali.

Tutte le componenti hardware e software del VSS sono sottoposte a regolare aggiornamento a cura di personale specializzato autorizzato.

2. ORGANIZZAZIONE

2.1 Ruoli, funzioni e responsabilità

Vengono di seguito definiti ruoli con relative funzioni e responsabilità dei soggetti coinvolti nei processi di gestione del VSS.

RUOLO	FUNZIONI E RESPONSABILITA'
Titolare del trattamento (ex art.4 GDPR)	Fanno capo al Titolare tutti gli obblighi ed i poteri previsti dalla legge, finalizzati a garantire che il trattamento avvenga nel rispetto dei principi posti a tutela dei diritti degli interessati. In particolare, competono al Titolare: <ul style="list-style-type: none"> - determinare le finalità e i mezzi del trattamento; - individuare i tempi di conservazione delle immagini; - individuare e incaricare i Delegati al trattamento; - verificare periodicamente la protezione dei dati personali (coadiuvato dal DPO).
Responsabile interno del trattamento (Designato)	Competono al Responsabile interno designato: <ul style="list-style-type: none"> - valutare la legittimità del trattamento, rispetto alle modalità con cui questo viene svolto; - individuare gli operatori interni autorizzati alle operazioni di trattamento definendone gli specifici profili di abilitazione; - inserire e aggiornare il trattamento nel registro dei

	<p>trattamenti d'Ateneo;</p> <ul style="list-style-type: none"> – vigilare sulla conservazione delle immagini e sulla loro cancellazione nei termini previsti dal presente Disciplinare; – verificare le attività dei fornitori esterni, in riferimento alle regole ed istruzioni impartite contrattualmente nell'atto di designazione a Responsabile esterno del trattamento ex art. 28 GDPR; – autorizzare, in affiancamento al Titolare del trattamento, le operazioni di accesso alle immagini, anche registrate, e la produzione di eventuali copie; – effettuare preventiva valutazione del rischio per la libertà e la dignità delle persone in ambito di protezione dati personali nei casi previsti, informando il Titolare nei casi in cui il trattamento comporti un rischio elevato non mitigabile; – Tenere i rapporti con le Autorità.
Responsabile esterno del trattamento (ex art. 28 GDPR)	<p>Le funzioni e le competenze del Responsabile esterno del trattamento sono definite da AGIS nell'atto di designazione tenuto anche conto di quanto previsto dal contratto di affidamento dello specifico servizio.</p> <p>Al Responsabile esterno del trattamento compete esclusivamente l'identificazione degli Autorizzati al trattamento di secondo livello.</p>
Autorizzato al trattamento (ex art. 29 GDPR)	<p>È il personale (interno o esterno all'Ateneo), distinto in Autorizzato al trattamento di primo livello e Autorizzato al trattamento di secondo livello, che effettua materialmente le operazioni di trattamento dei dati. Più specificamente, i compiti sono così distribuiti:</p> <p>Autorizzato al trattamento di primo livello:</p> <ul style="list-style-type: none"> – autorizzare, in affiancamento al Responsabile interno del trattamento, le operazioni di accesso alle immagini, anche registrate, e la produzione/comunicazione di eventuali copie; – presidiare i rapporti con l'autorità di contrasto (polizia giudiziaria). <p>Autorizzato al trattamento di secondo livello:</p> <ul style="list-style-type: none"> – visionare le immagini in tempo reale; – accogliere le richieste di accesso alle immagini (ferma restando la facoltà degli interessati di rivolgersi direttamente al Titolare, al Responsabile interno del trattamento ed agli Autorizzati di primo livello); – effettuare ricerche, estrazioni e custodia di eventuali copie di immagini nei casi consentiti ed autorizzati; – comunicare i dati ai soggetti legittimati/autorizzati. <p>L'Autorizzato al trattamento, nello svolgimento delle operazioni strettamente connesse all'adempimento delle proprie funzioni, deve attenersi scrupolosamente alle istruzioni impartite dal proprio responsabile diretto, impegnandosi ad adottare tutte le misure di sicurezza previste dal presente Disciplinare nonché ogni altra misura idonea ad</p>

	evitare la comunicazione o la diffusione non autorizzata dei dati ed il rischio, anche accidentale, di distruzione, perdita o accesso non conforme alle finalità perseguite.
Amministratore di sistema	<p>È il personale tecnico (interno o esterno all'Ateneo), preposto a sovrintendere alla componente informatica del VSS, al quale sono affidate le attività di:</p> <ul style="list-style-type: none"> – installazione, configurazione e manutenzione delle telecamere e delle risorse informatiche correlate al funzionamento del VSS; – assegnazione e custodia delle credenziali di accesso necessarie per l'utilizzo degli impianti di videosorveglianza. <p>È soggetto alla specifica disciplina del Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e s.m.i.</p>
Responsabile della Protezione dei Dati (ex art. 37 GDPR)	<p>Il DPO ha un ruolo consultivo. Affianca il Titolare ed il Responsabile del trattamento con funzioni di supporto, controllo e prassi formative e informative sulle disposizioni previste dal GDPR.</p> <p>In particolare, ha il compito di:</p> <ul style="list-style-type: none"> – informare il Titolare ed i Responsabili, nonché i soggetti Autorizzati circa gli obblighi previsti in materia di privacy; – se richiesto, fornire parere al Titolare in merito alla valutazione d'impatto dei trattamenti sulla protezione dei dati e sorvegliare i relativi adempimenti; – cooperare con l'Autorità di controllo; – fungere da punto di contatto con i soggetti interessati in merito a qualsiasi problematica dovesse emergere riguardo ai trattamenti dei dati.

2.1.1 Titolare del trattamento

Il Titolare del trattamento è il Politecnico di Milano con sede in P.zza Leonardo da Vinci 32, 20133 - Milano in persona del Direttore Generale su delega del Rettore pro-tempore; per esercitare in concreto i suoi poteri, esso si avvale delle figure individuate nei successivi paragrafi.

2.1.2 Responsabile interno del trattamento (Designato)

In relazione al trattamento di cui al Disciplinare, il Responsabile interno del trattamento è il dirigente dell'Area Gestione e Infrastrutture del Politecnico di Milano.

2.1.3 Responsabili esterni del trattamento

In relazione al trattamento di cui al Disciplinare, i Responsabili esterni del trattamento sono le società fornitrici dei servizi di portierato, Control Room e assistenza tecnica specialistica sul VSS contrattualizzate da AGIS e da ASICT.

I Responsabili esterni del trattamento sono elencati nel registro dei trattamenti (ex art. 30 GDPR).

2.1.4 Autorizzati al trattamento

I soggetti Autorizzati al trattamento di cui al presente Disciplinare sono:

- a. I dipendenti del Titolare del trattamento, autorizzati dal Responsabile interno del trattamento in ragione dello specifico ruolo e funzione.
- b. I dipendenti del Responsabile esterno del trattamento, nei limiti del profilo di autorizzazione assegnato. Il Responsabile esterno del trattamento redige e rende disponibile al Titolare del trattamento l'elenco nominativo dei propri dipendenti autorizzati al trattamento.

2.1.5 Amministratori di sistema

Gli Amministratori di sistema competenti in relazione al VSS oggetto del Disciplinare sono individuati tra i tecnici dell'Area Servizi ICT del Politecnico di Milano.

Gli Amministratori di sistema sono elencati nel registro dei trattamenti (ex art. 30 GDPR).

2.1.6 Responsabile della Protezione dei Dati

Il DPO è reperibile presso l'Ufficio del Responsabile della Protezione dei Dati del Politecnico di Milano (contatto: privacy@polimi.it).

3. DISPOSIZIONI

3.1 Principi generali del trattamento

La videosorveglianza, applicata laddove altre misure di protezione non siano sufficienti, attuabili o parimenti efficaci, viene condotta secondo i principi generali di seguito elencati:

- a. Per finalità determinate, esplicite e lecite. In particolare, i dati raccolti dal sistema di videosorveglianza:
 - non sono utilizzati per scopi diversi da quelli dichiarati dal Titolare oppure comunicati/diffusi a terzi, salvo che agli organi giudiziari e di polizia giudiziaria, per il tramite del Titolare del trattamento e dei soggetti dallo stesso espressamente individuati;
 - possono essere rilasciati a soggetti privati, per la tutela di un diritto non immediatamente riconducibile alle finalità perseguite dal Titolare del trattamento, solo a seguito di ordine degli organi giudiziari e di polizia giudiziaria;
 - possono essere utilizzati, ai fini del perseguimento delle finalità dichiarate dal Titolare del trattamento, in sede di giudizio civile o penale, per agevolare l'esercizio del diritto di difesa del Titolare stesso.
 - Nel rispetto del principio di pertinenza e non eccedenza del trattamento, con numero/dislocazione/modalità di ripresa delle telecamere e funzionalità del VMS stabiliti in modo da consentire la raccolta delle sole immagini necessarie al raggiungimento delle finalità perseguite;
- b. In modo che gli interessati, attraverso l'informativa ex artt. 13 e 14 del GDPR nonché mediante opportuna segnaletica di avvertimento, siano messi a conoscenza dell'applicazione della videosorveglianza e delle finalità perseguite, così da poterne verificare la liceità in base alla vigente normativa ed esercitare i diritti contemplati dagli artt. da 15 a 22 e 77 del GDPR.
- c. Nel rispetto del divieto di controllo a distanza dei lavoratori e delle garanzie previste al riguardo (ex art. 4 della legge 300/1970).
- d. Nel rispetto del principio di minimizzazione del dato ossia per il tempo strettamente necessario alla finalità nel caso particolare perseguita.
- e. Previa individuazione, autorizzazione e istruzione dei soggetti che possono utilizzare gli impianti, adottando procedure atte a garantire, attraverso profili diversificati, l'accesso alle immagini e la realizzazione di copie delle registrazioni esclusivamente ai soggetti autorizzati. In particolare, gli incaricati alla videosorveglianza sono:
 - in numero limitato, identificati nominativamente e assegnatari di specifici profili di autorizzazione, tali da consentire l'esecuzione delle sole operazioni necessarie e sufficienti all'assolvimento dei propri compiti e la tracciabilità delle stesse;
 - soggetti all'autorità diretta del Titolare del trattamento ovvero del Responsabile del trattamento, secondo l'organizzazione di appartenenza e gli incarichi assegnati;
 - vincolati all'obbligo di riservatezza.
- f. In modo che i tecnici installatori e manutentori del sistema di videosorveglianza (in qualità di Amministratori di sistema) possano avere accesso al sistema per garantirne il corretto funzionamento esclusivamente nei limiti e in ragione delle operazioni strettamente necessarie.
- g. In modo tale che la trasmissione in rete, la registrazione e l'accesso visivo delle immagini siano protette da misure di sicurezza idonee ad evitare eventuali rischi di perdita, distruzione, accesso non autorizzato, trattamento illecito o difforme alle finalità perseguita.

3.2 Finalità del trattamento

Il Politecnico di Milano effettua attività di videosorveglianza:

- a. Per finalità di tutela del patrimonio dell'Ateneo da atti vandalici, danneggiamenti e furti.
- b. Per favorire la sicurezza e l'incolumità fisica del personale universitario, degli studenti e dei frequentatori legittimati, a vario titolo, ad accedere agli spazi universitari.
- c. Al fine di prevenire e rilevare accessi illeciti e non autorizzati agli spazi di pertinenza dell'Ateneo (luoghi ad alto rischio, infrastrutture IT, ecc.).
- d. Per necessità investigative dell'Autorità giudiziaria o delle Forze dell'Ordine.

3.3 Base giuridica del trattamento

In merito alle finalità "a", "b", "c" di cui al paragrafo precedente, la base giuridica del trattamento di dati personali relativi alla videosorveglianza è costituita dall'art. 6, par. 1, lett. e) del GDPR (interesse pubblico).

In merito alla finalità "d" del paragrafo precedente, la base giuridica del trattamento di dati personali relativi alla videosorveglianza è costituita dall'art. 6, par. 1, lett. c) del GDPR (obbligo legale).

3.4 Impatto del trattamento

Considerate le modalità attraverso cui si perseguono le finalità richiamate ed in particolare:

- che la dislocazione, l'orientamento, l'angolo di ripresa e la risoluzione delle telecamere sono valutati con esclusivo riferimento alle suddette finalità, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità stesse, in modo da non interferire con le attività di studio, lavoro e ricerca svolte in Ateneo, nel rispetto dei principi di pertinenza e non eccedenza;
 - che i dati possono essere consultati solo da personale appositamente autorizzato e dotato di utenze secondo profili diversificati che ne consentono l'identificazione e la tracciabilità delle operazioni;
 - che sono stati definiti e configurati tempi massimi per la conservazione delle immagini, individuando modalità per la gestione delle eventuali copie off-site da realizzarsi su ordine di una autorità competente;
 - che sono state individuate modalità e procedure per consentire agli interessati l'esercizio dei diritti previsti dal GDPR;
 - che il sistema di videosorveglianza non è connesso direttamente o indirettamente con banche dati esterne, anagrafiche o biometriche;
 - che non vengono impiegate funzioni di video-analitica avanzata;
 - che il trattamento dei dati effettuato non è qualificabile come trattamento "su larga scala";
- si ritiene che non sussista l'esigenza di effettuare specifica "Valutazione di impatto sulla protezione dei dati" (DPIA) ai sensi dell'art. 35 GDPR ovvero che il trattamento non costituisca, anche in ragione delle misure di sicurezza previste e descritte nel Disciplinare, un rischio elevato per i diritti e le libertà delle persone interessate.

Qualora, in caso di variazione delle modalità del trattamento, si modifichi il profilo di rischio per i diritti e le libertà degli interessati, il Titolare del trattamento procederà di conseguenza ad un riesame della valutazione d'impatto sulla protezione dei dati.

3.5 Durata di conservazione delle registrazioni

In conformità dei principi di minimizzazione dei dati e di limitazione della loro conservazione di cui all'art. 5, par. 1, lettere c) ed e) del GDPR, le registrazioni del VMS sono conservate per 72 ore dalla ripresa (salvo ulteriore conservazione nei periodi di chiusura dell'Ateneo, nonché per richiesta dell'Autorità giudiziaria o di Polizia giudiziaria).

Solo in caso di sospetta o evidente notizia di danno o di reato, le immagini estrapolate su espressa richiesta del soggetto che abbia sporto denuncia/querela, può essere protratta per un massimo di 15 giorni naturali e consecutivi nell'attesa che l'Autorità procedente le richieda.

Decorso i termini di conservazione, le immagini sono cancellate automaticamente ed irreversibilmente.

3.6 Informativa trattamento dati personali

In conformità alle disposizioni di cui all'art. 13 GDPR, allo specifico Provvedimento a carattere generale del Garante del 8 aprile 2010 ed alle Linee Guida 3/2019 dell'EDP, si è proceduto alla predisposizione dell'informativa semplificata (segnaletica di avvertimento collocata in posizione chiaramente visibile prima del raggio d'azione della telecamera) e dell'informativa estesa (dettagliata e completa); quest'ultima pubblicata nell'apposita sezione Privacy del sito istituzionale dell'Ateneo.

3.7 Esercizio dei diritti dell'interessato

L'interessato al trattamento (soggetto ripreso identificabile) potrà esercitare, nei confronti dell'Ateneo, i diritti previsti dal GDPR e precisamente:

- diritto di accesso ai dati personali ed alle informazioni ai sensi dell'art. 15 del GDPR;
- diritto di opposizione al trattamento dei propri dati personali, fermo quanto previsto in relazione alla necessità di obbligatorietà del trattamento dati per poter fruire dei servizi offerti;
- diritto di limitazione del trattamento ai sensi dell'art. 18 del GDPR;
- diritto alla cancellazione (diritto all'oblio) dei propri dati, fatta eccezione per quelli contenuti in atti che devono essere obbligatoriamente conservati dal Politecnico di Milano e salvo che sussista un motivo legittimo prevalente per procedere al trattamento.

In considerazione della natura intrinseca dei dati trattati (immagini raccolte in tempo reale), non è in concreto esercitabile il diritto di aggiornamento o integrazione, nonché il diritto di rettifica di cui all'art. 16 del GDPR. Non è altresì esercitabile il diritto alla portabilità dei dati di cui all'art. 20 del GDPR in quanto le immagini acquisite con il sistema di videosorveglianza non possono essere trasferite a soggetti terzi a quelli espressamente autorizzati e che, operando sotto la diretta autorità del Titolare o del Responsabile del trattamento.

L'interessato identificabile, potrà richiedere l'accesso visivo alle registrazioni nelle quali ritiene di essere stato ripreso (allegando all'istanza idoneo documento di riconoscimento). La risposta a una richiesta di accesso non potrà tuttavia in alcun modo comprendere eventuali dati riferiti a soggetti terzi rispetto alla parte istante (a tal fine, è altresì esclusa la possibilità di applicare trattamenti di scomposizione o di mascheramento selettivo dei fotogrammi).

L'istruttoria e la conseguente decisione sul riconoscimento del diritto vantato dall'interessato sono di competenza del Responsabile interno del trattamento.

Per l'esercizio dei soli diritti di accesso alle registrazioni video, nonché per ogni eventuale informazione, l'interessato può rivolgersi al Contact Center del Politecnico di Milano (contatto: contactcenter@polimi.it - tel. 02 2399 9300). Nel caso di esercizio dei succitati diritti di opposizione, limitazione e cancellazione sul trattamento dei dati personali, l'interessato può rivolgersi al DPO del Politecnico di Milano (contatto: privacy@polimi.it).

L'interessato al trattamento ha inoltre diritto di proporre reclamo alle competenti autorità di controllo, ovvero l'Autorità Garante per la protezione dei dati personali (www.garanteprivacy.it).

4. PROCESSI E PROCEDURE

Vengono di seguito descritti i processi e le procedure principali di conduzione del VSS.

4.1 Realizzazione, modifica e dismissione degli impianti di videosorveglianza

Il ciclo di vita dell'impianto di videosorveglianza tipo è articolato nelle seguenti fasi principali:

- a. La necessità e i requisiti funzionali degli impianti di videosorveglianza sono stabiliti da AGIS sulla base delle finalità individuate dal Titolare, coerentemente con le policies di sicurezza di Ateneo.
- b. ASICT formula un parere tecnico di fattibilità e stabilisce la soluzione tecnologica più idonea in base alle finalità espresse.
- c. Ove la soluzione tecnologica presenti elementi di criticità in materia di protezione dei dati personali, viene informato il DPO di Ateneo.

- d. ASICT è responsabile dei procedimenti di installazione e configurazione e manutenzione del VSS nella sua interezza (dispositivi di ripresa, infrastruttura informatica di trasmissione, elaborazione ed archiviazione dati).
- e. Successivi interventi di modifica dell'impianto in termini di consistenza (numero di telecamere) e configurazione (puntamento/angolo di visuale, risoluzione/frame rate, periodo di conservazione delle registrazioni, ecc.) sono autorizzati da AGIS e vengono effettuati da ASICT valutata la conformità tecnica e normativa (consultato eventualmente il DPO) delle modifiche richieste.
- f. AGIS aggiorna la documentazione informativa e la segnaletica nei casi di realizzazione/modifica/dismissione degli impianti.
- g. Modifiche/dismissioni di impianti potranno essere attivate d'ufficio da ASICT per comprovate ragioni di obsolescenza tecnologica e/o di sicurezza informatica.

4.2 Accesso alle immagini in tempo reale

L'accesso ai flussi video live provenienti dalle telecamere avviene mediante postazioni client del VMS con abilitazioni di sola visualizzazione, ubicate nelle principali portinerie di campus (dove sono visualizzate esclusivamente le telecamere degli edifici di pertinenza) e nella Control Room di Ateneo (dove sono visualizzate tutte le telecamere dell'impianto).

Si precisa che le postazioni client di monitoraggio non sono abilitate alla visualizzazione differita delle immagini registrate né dispongono di funzioni di modifica e zoom dell'inquadratura (l'inquadratura e il livello di zoom applicato sono predefiniti e bloccati dall'Amministratore del sistema in fase di installazione della singola telecamera).

Dette postazioni sono presidiate da operatori Autorizzati al trattamento, dipendenti da società designate come Responsabile esterno del trattamento nell'ambito dei contratti di servizi.

4.3 Trattamento delle immagini registrate

L'accesso alle registrazioni video, per motivi di comprovata necessità (a titolo esemplificativo, in occasione di eventi lesivi del patrimonio dell'Ateneo), avviene all'interno della sede del Titolare del trattamento, attraverso postazioni client del VMS con abilitazioni di secondo livello (visualizzazione, ricerca e copia delle immagini registrate), accessibili esclusivamente a personale autorizzato.

Le operazioni di trattamento si suddividono in:

- **Consultazione visiva delle registrazioni;**
- **Copia delle registrazioni.**

4.3.1 Consultazione visiva delle immagini registrate

La consultazione visiva delle immagini registrate è consentita esclusivamente ai seguenti soggetti:

- al Titolare del trattamento;
- al Responsabile interno del trattamento e/o ai soggetti Autorizzati al trattamento di primo livello;
- al personale esterno Autorizzato al trattamento di secondo livello (con specifico profilo di autorizzazione) solo per provvedere alle operazioni autorizzate di ricerca, salvataggio e creazione di copie;
- all'Autorità giudiziaria ed alle Forze dell'Ordine (per indagini in corso, per attività finalizzate alla tutela di un diritto in giudizio o per attività di prevenzione e repressione di illeciti).

4.3.2 Conservazione di copie delle immagini

Le immagini estratte potranno essere conservate in modalità on-site oppure in modalità off-site:

- **Conservazione on-site.** Le immagini vengono copiate in un'apposita area predisposta sullo storage del VSS. per il tempo strettamente necessario alla comunicazione al richiedente.
- **Conservazione off-site.** Le immagini vengono copiate su supporti di memorizzazione

esterni che dovranno essere custoditi in luogo protetto, con accesso riservato ai soggetti autorizzati per il tempo strettamente necessario alla consegna materiale al richiedente. I supporti di memorizzazione esterni saranno contrassegnati con:

- identificazione del soggetto richiedente (nome dell'autorità richiedente);
- data della richiesta;
- data e orario delle riprese;
- numero identificativo del relativo ticket di servizio AGIS.

Il file video riporteranno impressi l'identificativo della telecamera, data e l'ora dell'evento (saranno valorizzati, con apposita nota, eventuali scostamenti riscontrati in fase di estrazione tra l'ora reale e quella impressa sulle immagini dal sistema).

Il file sarà estratto di norma nel formato video standard (.MP4). Sono fatte salve specifiche ed espresse esigenze di analisi video forense per le quali il file sarà estratto nel formato proprietario del VMS Cathexis (.CAR) e corredato dell'apposito viewer.

Le copie delle immagini saranno conservate per un periodo massimo di 15 giorni naturali e consecutivi per consentirne la visione/estrazione di copia da parte dell'Autorità Giudiziaria o delle Forze dell'Ordine.

L'acquisizione di copie delle registrazioni, previa formale e motivata richiesta, è concessa esclusivamente ai seguenti soggetti:

- al Titolare del trattamento;
- al Responsabile interno del trattamento e/o ai soggetti Autorizzati al trattamento di primo livello;
- all'Autorità giudiziaria ed alle Forze dell'Ordine (per indagini in corso, per attività finalizzate alla tutela di un diritto in giudizio o per attività di prevenzione e repressione di illeciti);
- agli avvocati difensori per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria (art. 391-quarter Codice Procedura Penale), previa presentazione della documentazione comprovante il titolo di legittimazione richiesto.

4.3.3 Eliminazione delle copie delle immagini

Qualora, entro 15 giorni naturali e consecutivi a decorrere dalla richiesta di blocco, le immagini non vengano richieste dall'Autorità giudiziaria o dalle Forze dell'Ordine, tutte le copie saranno cancellate in modo irreversibile a cura dell'operatore incaricato del trattamento.

I supporti di memorizzazione esterni non riscrivibili contenenti copie di immagini e non ritirati dagli aventi diritto entro i tempi stabiliti saranno fisicamente distrutti dall'incaricato del trattamento.

Ai fini del riutilizzo controllato, i supporti di memorizzazione riscrivibili (es. pendrive o hard disk) saranno sottoposti a formattazione di basso livello, in modo da rendere impossibile il recupero di dati precedentemente memorizzati.

4.3.4 Processo di produzione e comunicazione di copie delle immagini registrate

Qualora un soggetto terzo ritenga di avvalersi di immagini per tutelare o esercitare un proprio diritto in giudizio, potrà richiedere in via cautelativa la conservazione temporanea di eventuali registrazioni utili. A tal fine, dovrà rivolgersi alle Autorità competenti, le quali ordineranno l'acquisizione delle registrazioni e/o la conservazione per un periodo superiore a quello predefinito dal sistema.

In pendenza di tale ordine, dovrà presentare alla Control Room AGIS formale richiesta scritta e motivata. La richiesta dovrà essere corredata da una copia della denuncia/querela o comunque dall'impegno a presentarla quanto prima.

A seguito della ricezione di istanza di accesso alle registrazioni, viene attivata la procedura descritta nei punti seguenti.

a. Accoglimento e valutazione preliminare dell'istanza

L'operatore della Control Room AGIS (Autorizzato al trattamento di secondo livello):

1. Riceve l'istanza di accesso e, se necessario, interagisce con il richiedente per ottenere ogni elemento utile a circostanziare le immagini oggetto dell'istanza:
 - luogo in cui è avvenuto l'evento;
 - data e ora specifiche o intorno temporale dell'evento;
 - motivo della richiesta.(Istanze non adeguatamente circostanziabili in termini temporali e spaziali o prive di motivazione, sono considerate irricevibili).
2. Genera un ticket di servizio per la gestione ed il tracciamento della richiesta di trattamento allegando tutte le informazioni e gli eventuali documenti ricevuti.
3. Si accerta dell'effettiva disponibilità di immagini utili a soddisfare la richiesta.
4. In caso di accertamento negativo, ne riferisce la motivazione al soggetto istante (es. le immagini sono state cancellate entro i tempi indicati nell'informativa) e chiude il ticket di trattamento.

b. Estrazione e copia delle immagini

L'operatore della Control Room AGIS (Autorizzato al trattamento di secondo livello):

5. Nel caso l'istanza di accesso alle registrazioni provenga da un soggetto implicitamente legittimato (Titolare del trattamento, Responsabile interno del trattamento e/o Autorizzato al trattamento di primo livello, Autorità giudiziaria o Forze dell'ordine) procede alle azioni del punto 12 e successivi della procedura.
6. Nel caso l'istanza provenga da un soggetto terzo, a condizione che siano disponibili immagini dello specifico luogo dell'evento e che sia chiaramente espressa la finestra temporale utile:
 - procede all'estrazione ed al salvataggio on-site sul sistema di una copia delle immagini (limitatamente a quelle pertinenti e non eccedenti i termini definiti con l'istanza);
 - notifica immediatamente l'istanza al Responsabile interno o all'Autorizzato al trattamento di primo livello e attende istruzioni per l'eventuale comunicazione delle copie.
7. Nel caso l'istanza provenga da un soggetto terzo, ove non siano disponibili immagini dello specifico luogo dell'evento oppure non siano definiti i termini temporali e comunque in caso di dubbi notifica immediatamente l'istanza al Responsabile interno o all'Autorizzato al trattamento di primo livello ed attende istruzioni per l'eventuale estrazione e comunicazione delle immagini.

c. Valutazione finale dell'istanza di accesso

Il Responsabile interno del trattamento e/o l'Autorizzato al trattamento di primo livello:

8. Pondererà la legittimità delle motivazioni prodotte a sostegno dell'istanza, eventualmente avvalendosi del supporto del DPO e dell'Ufficio Legale, stabilendo se accogliere o respingere l'istanza di accesso alle registrazioni.
9. In caso di palese violazione delle finalità previste per il trattamento oppure di indisponibilità di immagini utili, rigetta l'istanza dandone motivazione all'interessato ed aggiorna il ticket del trattamento.
10. In caso di accoglimento dell'istanza, comunica alla Control Room AGIS, tramite nota sul ticket di trattamento, l'autorizzazione e le indicazioni per il trattamento (definendo quantità e durata dei flussi video da estrapolare).

Le copie delle immagini estratte verranno custodite dall'Autorizzato al trattamento per 15 giorni naturali e consecutivi dalla loro produzione oppure per tutto il tempo intercorrente tra la richiesta di conservazione formulata dall'Autorità giudiziaria o dalle Forze dell'ordine e la consegna materiale.

d. Comunicazione delle copie/cancellazione dei dati.

L'operatore della Control Room AGIS (Autorizzato al trattamento di secondo livello):

11. Ove sia stata negata la comunicazione delle immagini, provvede alla

cancellazione/distruzione di tutte le eventuali copie predisposte e chiude il ticket del trattamento.

12. Ove sia stata autorizzata la comunicazione delle immagini, realizza la copia delle registrazioni su supporti di memorizzazione esterni assicurandosi dell'integrità dei supporti.
13. Concorda con il richiedente le modalità del rilascio delle copie.
14. Consegna al richiedente la copia delle registrazioni, allegando al ticket del trattamento il verbale di consegna o quantomeno gli estremi della consegna (data e nominativo del ricevente).
15. Attende 5 giorni naturali e consecutivi affinché il richiedente si assicuri che le copie fornite siano complete e integralmente fruibili, trascorsi i quali, in assenza di indicazioni contrarie, provvede alla distruzione delle copie conservate on-site ed alla chiusura il ticket del trattamento.

4.4 Registrazione degli accessi al VSS

Gli accessi ai dati contenuti nel VSS, per operazioni di consultazione visiva e/o estrazione di copie delle registrazioni (compresi gli accessi per richieste a cui si è dato riscontro negativo) saranno registrati e controllati.

Il registro degli accessi al sistema di videosorveglianza oggetto di questo Disciplinare è sostanzialmente e concretamente costituito dal database dell'applicazione di service ticketing (OTOBO/OTRS) utilizzata sia per la gestione delle richieste di accesso alle immagini che per il tracciamento delle attività tecniche di manutenzione ordinaria e straordinaria del VSS.

Nel ticket di servizio saranno riportati dall'Autorizzato al trattamento (quando non ricavabili implicitamente dagli attributi del ticket stesso):

- motivazione dell'accesso (corredata dalla documentazione prodotta dal richiedente);
- nominativo del richiedente l'accesso;
- data e l'ora dell'accesso;
- nominativo dell'operatore che ha effettuato l'accesso;
- estremi delle immagini visionate (identificativo della telecamera ed intervalli temporali delle registrazioni video trattate);
- riferimenti relativi all'eventuale avvenuta consegna di copie delle immagini.

La compilazione del registro degli accessi rientra nei compiti degli operatori Autorizzati di secondo livello allo specifico trattamento mentre il controllo e la messa a disposizione dello stesso è compito del Responsabile interno del trattamento.