

Disposizioni relative alla gestione del sistema di videosorveglianza

del 26.01.2026 (stato al 24.08.2026)

Tenuto conto e in virtù del quadro normativo applicabile, in particolare di quanto previsto nel Regolamento generale sulla videosorveglianza all'Università della Svizzera italiana (in seguito, il "Regolamento"), in particolare all'art. 3, nonché nella Legge cantonale sulla protezione dei dati personali (la "LPDP") e nella Legge cantonale sulla videosorveglianza pubblica (la "LVISO"),

Il Rettorato adotta:

Art. 1 **Oggetto** **e finalità**

- ¹ Le presenti Disposizioni concretizzano ed eseguono il Regolamento, e disciplinano le procedure interne vincolanti per la gestione tecnica e organizzativa, da parte del Titolare dell'elaborazione (cfr. art. 2 cpv. 1, lett. a), del sistema di videosorveglianza presente presso le Sedi universitarie (cfr. art. 2 cpv. 1, lett. h), al fine di garantire la sicurezza di persone e beni, nel rispetto della protezione dei dati personali e dei diritti dei collaboratori, della comunità universitaria e, in generale, dell'utenza.
- ² Conformemente a quanto previsto all'art. 1 del Regolamento, il sistema di videosorveglianza in modalità dissuasiva dell'Università della Svizzera italiana (di seguito "USI" o "l'Università") è finalizzato esclusivamente a:
 - a. tutelare la vita, l'integrità fisica e gli altri beni giuridici degli utenti delle Sedi universitarie;
 - b. proteggere i beni e le infrastrutture universitarie;
 - c. prevenire e accertare la commissione di eventi illeciti;
 - d. gestire eventuali situazioni di emergenza che coinvolgano beni giuridici rilevanti tutelati dall'ordinamento giuridico, e
 - e. in casi chiaramente definiti, USI opera la videosorveglianza in modalità invasiva per gestire l'accesso a beni amministrativi o a strutture gestiti dall'USI, o assicurarne la logistica.
- ³ È escluso qualsiasi utilizzo del sistema di videosorveglianza dell'Università per finalità diverse o incompatibili con quelle sopra indicate.

Art. 2 **Definizioni**

- ¹ Ai fini delle presenti Disposizioni si intende per:
 - a. "Titolare dell'elaborazione": l'Università della Svizzera italiana (USI), con sede in Via G. Buffi 13, 6900 Lugano, Svizzera;

- b. "Responsabile interno": la figura interna al Titolare dell'elaborazione incaricata della gestione delle strutture, nell'ambito delle quali sono elaborati i dati personali per le finalità istituzionali; in particolare il Servizio logistica e sicurezza dell'Università, rappresentato dal proprio Responsabile di Servizio. Nelle questioni ordinarie maggiormente operative, il Responsabile interno è coadiuvato dallo "Specialista salute e sicurezza", figura definita nell'**Allegato 2** alle presenti Disposizioni. Si tratta di un collaboratore del Servizio logistica e sicurezza dell'Università incaricato di gestire la prevenzione degli infortuni, la protezione della salute e la sicurezza nelle Sedi universitarie;
 - c. "Amministratore di sistema": una o più persone fisiche individuate nell'ambito del Servizio informatico dell'Università (di seguito "Servizio IT"), incaricate della gestione e della manutenzione del sistema informatico o di sue componenti. Rientrano in tale definizione anche le figure equiparabili, sotto il 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, nonché gli amministratori di sistemi software complessi;
 - d. "Personale autorizzato": la persona fisica (o le persone fisiche) autorizzata/e dal Responsabile interno a compiere operazioni di elaborazione dei dati nell'ambito della gestione del sistema di videosorveglianza dell'Università, nei ruoli e con i diritti indicati nell'**Allegato 2** alle presenti Disposizioni;
 - e. "Direzione": il gremio rappresentante il Titolare dell'elaborazione, composto collettivamente dal Rettore, dal Direttore operativo e/o dal Direttore operativo aggiunto, nonché dal Segretario generale dell'Università;
 - f. "CPD": il Consulente per la protezione dei dati in USI, figura di consulenza e supporto al Responsabile interno e alla Direzione nell'adempimento degli obblighi in materia di protezione dei dati personali;
 - g. "SLC": il Servizio legale e compliance dell'USI;
 - h. "Sedi universitarie": i campus universitari e i beni amministrativi gestiti o cogestiti sostanzialmente dal Titolare dell'elaborazione, indipendentemente dai rapporti di proprietà; in particolare, gli stabili e/o i Campus definiti nell'**Allegato 1** alle presenti Disposizioni;
 - i. "Guardianie": gli stabili e le infrastrutture presenti nelle Sedi universitarie, con accesso sorvegliato, come definiti nell'**Allegato 1 e 2** alle presenti Disposizioni;
 - j. "Evento": si tratta di un evento rilevato durante le attività di pattugliamento sulle Sedi universitarie, oppure segnalato da terze parti (collaboratori, studenti, utenti terzi, autorità) che porta a sospettare, presuppone o conferma la messa in discussione degli obiettivi perseguiti dalla videosorveglianza in USI, ai sensi del Regolamento delle presenti Disposizioni;
 - k. "Elaborazione": 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, quali, a titolo esemplificativo, 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 di dati personali;
-

-
- l. "Trasmissione": l'azione di rendere accessibile, comunicare, o trasmettere in qualsiasi forma, determinate Registrazioni della videosorveglianza e/o informazioni concernenti le medesime, a soggetti diversi dal Titolare dell'elaborazione e dal Personale autorizzato ai sensi delle presenti Disposizioni;
 - m. "Registrazioni della videosorveglianza": immagini o videoregistrazioni, registrate dalle telecamere della videosorveglianza e conservate nel sistema di gestione della videosorveglianza. Esse si suddividono, in base alla modalità di potenziale visualizzazione, in: "*Riprese live*" (visualizzazione a schermo in tempo reale), "*Playback*" (possibilità, al momento dell'accesso, di riprodurre porzioni limitate nel tempo delle Registrazioni più recenti), e "*Registrazioni*" in senso stretto.
 - n. "Misure di sicurezza": il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza idonee a garantire un livello adeguato di protezione dei dati personali, conformemente alla normativa vigente.

Art. 3
Principi
generali

- ¹ La raccolta, la registrazione, la conservazione, la trasmissione e, più in generale, l'utilizzo di immagini, nonché la gestione del sistema di videosorveglianza dell'USI, costituiscono attività di elaborazione di dati personali. Conseguentemente, tali attività sono sottoposte ai principi di legalità, finalità e proporzionalità, così come ad ogni altro principio e requisito legale applicabile in materia di elaborazione di dati personali sancito dal diritto vigente, in particolare dalla LPDP, dalla LViSo e dal Regolamento.
 - ² L'elaborazione di dati personali attraverso sistemi di videosorveglianza da parte del Titolare dell'elaborazione avviene esclusivamente nell'ambito dell'esercizio delle proprie funzioni istituzionali, al fine di garantire la sicurezza e l'incolumità delle persone appartenenti alla comunità universitaria e dei frequentatori degli spazi universitari, nonché di tutelare il patrimonio dell'Università o di terzi adibito a tale scopo.
 - ³ I sistemi informatici utilizzati per il trattamento dei dati acquisiti tramite le videocamere ubicate nelle Sedi universitarie sono configurati e gestiti nel rispetto dei principi di "*privacy by design*" e "*privacy by default*" conformemente alle normative applicabili in materia di protezione dei dati personali.
 - ⁴ Gli impianti di videosorveglianza dell'USI che acquisiscono dati personali sono utilizzati nel rispetto di misure di sicurezza tecniche e organizzative adeguate, conformemente alle direttive universitarie in materia di sicurezza informatica.
 - ⁵ In generale, ogni accesso da parte del Personale autorizzato al sistema di videosorveglianza dell'Università, nell'espletamento delle proprie mansioni, deve essere tracciabile, nominativo, verificabile e preventivamente autorizzato, nonché essere giustificato da un Evento concreto.
 - ⁶ È fatto divieto assoluto di sfruttare o configurare il sistema di videosorveglianza dell'USI al fine di:
 - a. utilizzare tecniche di riconoscimento facciale automatico;
 - b. attivare funzioni di tracciamento automatizzato delle persone;
 - c. svolgere analisi comportamentali automatiche;
 - d. visionare le riprese in diretta e/o le Registrazioni senza autorizzazione e in assenza di uno scopo specifico e legittimo.
-

Art. 4
Modalità di
videosorveglianza
e registro delle
videocamere

- ¹ Allo scopo di perseguire le finalità di cui al Regolamento e alle presenti Disposizioni, nel rispetto dei principi enunciati, l'Università adotta le seguenti modalità di videosorveglianza:
- a. Modalità dissuasiva:
 - i. è applicata in aree comuni aperte (segnatamente perimetri, piazze, parcheggi) locali e stabili in cui sono presenti beni giuridici e valori patrimoniali rilevanti delle Sedi universitarie allo scopo di prevenire, rilevare e, se del caso, perseguire la commissione di atti illeciti;
 - ii. non prevede l'impiego della funzione di registrazione audio delle videocamere. Qualora tale funzione fosse resa possibile dai sistemi informatici impiegati, deve essere disattivata;
 - iii. prevede l'utilizzo, ove opportuno, di maschere privacy per oscurare aree specifiche all'interno del campo visivo delle videocamere (segnatamente qualora le riprese interessino finestre, ingressi di abitazioni private o spazi non pertinenti).
 - b. Modalità invasiva:
 - i. è limitata alla gestione di accessi a specifiche strutture e aree delle Sedi universitarie (segnatamente ingressi, laboratori, parcheggi, biblioteche, locali tecnici, sale sport, nonché locali che presentano specifici rischi per gli utenti o che richiedono un pronto intervento);
 - ii. di regola, prevede la visualizzazione delle Riprese live in chiaro;
 - iii. non prevede l'impiego della funzione di registrazione audio delle videocamere. Qualora tale funzione fosse resa possibile dai sistemi informatici impiegati, deve essere disattivata.
- ² Il Responsabile interno, singolarmente o con il supporto dell'Amministratore di sistema, è tenuto a:
- a. classificare e documentare preventivamente ogni videocamera utilizzata nelle Sedi universitarie, incluse le Misure di sicurezza applicate;
 - b. tenere e aggiornare periodicamente un registro delle videocamere in uso nelle Sedi universitarie, delle valutazioni effettuate e delle misure adottate per garantire il rispetto dei principi di elaborazione di dati personali (segnatamente limiti di registrazione temporale, apposizione di maschere privacy fisse o movibili);
 - c. monitorare periodicamente l'uso e la sicurezza degli impianti di videosorveglianza, nonché dei sistemi informatici ad essi connessi;
 - d. valutare e, se del caso, adeguare periodicamente le configurazioni tecniche delle videocamere, allo scopo di adempiere i requisiti previsti dalla normativa vigente applicabile, verificarne la funzionalità e intervenire, laddove necessario, con misure di manutenzione ordinaria e straordinaria;
 - e. aggiornare il sistema di videosorveglianza e le relative componenti con le patch di sicurezza più recenti disponibili; e
 - f. aggiornare la segnaletica di riferimento, ai sensi dell'art. 6 cpv. 5 delle presenti Disposizioni.

Art. 5
Misure di tutela
della privacy

- ³ Al fine di garantire la tutela della privacy, tenendo in debita considerazione le esigenze di sicurezza, il Responsabile interno, coadiuvato dall'Amministratore di sistema, adotta misure di protezione adeguate in fase di adozione, installazione e manutenzione delle videocamere, al fine di
-

-
- evitare acquisizioni sproporzionate di dati e informazioni attraverso il sistema di videosorveglianza. Tali misure comprendono, segnatamente:
- a. l'apposizione di maschere privacy fisse o movibili sulle videocamere;
 - b. la riduzione della risoluzione massima delle videocamere;
 - c. la riduzione della durata di ripresa e/o tempi di registrazione;
 - d. l'eventuale disattivazione di sistemi di intelligenza artificiale ("IA") o funzionalità analoghe installati direttamente sui dispositivi;
 - e. la disabilitazione delle funzioni di registrazione audio delle videocamere;
 - f. la disabilitazione delle funzioni PTZ (Pan – Tilt – Zoom) delle videocamere.
- ⁴ Il Responsabile interno provvede all'acquisto del materiale destinato alla videosorveglianza. Inoltre, egli verifica e garantisce che vengano fornite le specifiche attestazioni e certificazioni tecniche nel rispetto dei principi "privacy by default" e "privacy by design", nonché in conformità alla LPDP, LPD e alla LViSo.
- ⁵ Il Responsabile interno, con il supporto dell'Amministratore di sistema, adotta misure tecniche avanzate idonee a garantire la corretta gestione e conservazione delle Registrazioni, tra cui:
- a. la crittografia del media database del sistema di gestione della videosorveglianza;
 - b. l'uso di connessioni sicure; e
 - c. l'implementazione di un sistema efficace di autenticazione per l'accesso al sistema.
- ⁶ Il Responsabile interno definisce e adotta adeguate misure organizzative per implementare le procedure descritte nelle presenti Disposizioni, nonché per regolare e limitare gli accessi dei membri del Personale autorizzato.
-

Art. 6
Informazione
degli interessati
e segnaletica

- ¹ L'USI si impegna a garantire un'adeguata informazione alla comunità universitaria e ai visitatori delle Sedi universitarie mediante l'apposizione di segnaletica (segnatamente cartelli di avviso) ben visibile in prossimità delle aree videosorvegliate.
- ² Tale segnaletica, riporta un'informativa semplificata e indica come minimo:
- a. la presenza della videosorveglianza;
 - b. il Titolare dell'elaborazione (USI);
 - c. la base legale di riferimento; e
 - d. il rinvio all'informativa estesa sulla videosorveglianza dell'USI (cfr. cpv. 5).
- ³ Il supporto segnaletico di cui al cpv. 1:
- a. è collocato prima del raggio di azione della videocamera in questione, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
 - b. presenta un formato ed un posizionamento tale da risultare chiaramente visibile in ogni condizione di illuminazione ambientale, anche qualora il sistema di videosorveglianza sia attivo in orario notturno;
 - c. può includere un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare l'utenza se le immagini sono solo visionate o anche registrate dalle videocamere.
- ⁴ A complemento di quanto previsto ai cpv. 1-3, il Titolare dell'elaborazione provvede a richiamare l'attenzione delle persone interessate in modo più
-

capillare anche tramite apposizione di cartelli maggiormente semplificati, che contengano almeno il contenuto di cui al cpv. 2 lett. a e lett. d.

- ⁵ Il Responsabile interno cura e monitora l'affissione, la regolarità e la manutenzione dei supporti segnaletici di cui ai capoversi precedenti. Provvede inoltre, con il supporto del CPD, a mettere a disposizione dell'utenza l'informativa estesa relativa al sistema di videosorveglianza presente nelle Sedi universitarie (segnatamente tramite pubblicazione sul sito internet dell'USI). L'informativa estesa contiene le informazioni specifiche e complete previste dalla normativa applicabile.

Art. 7
Ruoli operativi,
responsabilità e
processo
d'autorizzazione

- ¹ La visualizzazione e l'accesso a fini operativi del Responsabile interno e, in generale, dei collaboratori e degli organi dell'USI alle Registre della videosorveglianza è strettamente limitato ai ruoli e profili autorizzati, come definiti nell'**Allegato 2** alle presenti Disposizioni. Tale accesso è implementato attraverso un sistema di controllo degli accessi e di configurazione nel sistema adottato, con attribuzione di privilegi granulari.
- ² Il Responsabile interno, rispettivamente l'Amministratore di sistema (quest'ultimo limitatamente ai membri del personale posto sotto la sua responsabilità), designa e autorizza per iscritto i membri del Personale autorizzato addetti alle attività di gestione della videosorveglianza, rispettivamente ai provvedimenti di natura informatica e di sicurezza IT, che ricoprono i ruoli e i profili definiti nell'**Allegato 2**. Prima di procedere all'assegnazione del ruolo dei collaboratori in parola, il Responsabile interno e l'Amministratore di sistema sono tenuti a:
- a. effettuare adeguati controlli di sicurezza riguardo al background dei membri del Personale autorizzato; per quanto concerne le Guardianie, il Responsabile interno può delegare tale competenza al Responsabile della Guardiania impartendo le necessarie istruzioni;
 - b. fornire per iscritto, ai membri del Personale autorizzato posti sotto la propria responsabilità, le istruzioni relative al trattamento e alla conservazione dei dati (incluso il luogo dove sono autorizzati a svolgere le loro attività), alla loro protezione contro eventuali rischi di violazione, e, in generale, circa il contenuto delle presenti Disposizioni. Tali istruzioni sono aggiornate in caso di modifiche tecniche, normative e organizzative;
 - c. far previamente sottoscrivere ai membri del Personale autorizzato, un impegno di confidenzialità. Il Responsabile interno e l'Amministratore di sistema (quest'ultimo limitatamente ai membri del personale posto sotto la sua responsabilità) possono esentare da tale obbligo i collaboratori amministrativi che, in base al Regolamento organico / CCL per il personale amministrativo, bibliotecario, tecnico e ausiliario dell'Università della Svizzera italiana, già sottostanno a tale obbligo;
 - d. assicurare che i membri del Personale autorizzato abbiano ricevuto una formazione idonea sulla protezione dei dati, sulle procedure operative e sulle responsabilità legali derivanti da un uso improprio del sistema di videosorveglianza, provvedendo ai necessari aggiornamenti periodici.
- ³ L'eventuale delega di compiti di sorveglianza a responsabili dell'elaborazione esterni all'USI è subordinata alla conclusione di una convenzione scritta tra il Titolare dell'elaborazione e tali persone incaricate esternamente, previa debita e ragionevole documentazione da parte del Responsabile interno della possibilità del partner contrattuale di adempiere ai requisiti regolamentari e contrattuali applicabili e/o stabiliti da USI.
-

Art. 8
Privilegi di sistema

- ¹ Il sistema di gestione della videosorveglianza dell'USI deve consentire la creazione di account utente individuali per i membri del Personale autorizzato, garantendo che ogni accesso sia riconducibile a una persona specifica.
- ² L'assegnazione di ruoli e privilegi al Personale autorizzato avviene a livello di singolo utente fisico, fatta eccezione per la gestione di tutte o parte delle Guardianie, come meglio specificato nell'**Allegato 2**, e a condizione che il Responsabile interno adotti misure organizzative atte a garantire la tracciabilità e la sicurezza del sistema.
- ³ In caso di necessità, il sistema deve permettere un'approvazione "caso per caso", attivando, a favore di persone eccezionalmente autorizzate, temporaneamente i privilegi necessari (segnatamente attraverso la creazione di ruoli utente temporanei) o verificando e, se del caso, adeguando i privilegi già attribuiti a richiedenti, membri del Personale autorizzato, nel sistema utilizzato, limitatamente alla durata autorizzata.
- ⁴ I privilegi assegnati sotto il profilo tecnico e/o organizzativo al Personale autorizzato, come meglio specificati all'**Allegato 2**, possono cumulativamente o alternativamente includere, a seconda dei ruoli:
 - a. la visualizzazione delle Riprese live (da postazione personale fissa o semifissa);
 - b. la visualizzazione delle Riprese live e in chiaro (da posizione di Guardiania fissa);
 - c. la visualizzazione di Playback, per le durate definite nell'**Allegato 2**;
 - d. la visualizzazione delle Registrazioni (da postazione personale fissa o semifissa);
 - e. la disponibilità di un telefono cellulare di servizio con accesso sicuro al sistema di videosorveglianza (durante il servizio di ronda);
 - f. la rimozione di eventuali maschere privacy mobili, da postazione fissa o semifissa, in caso di necessità;
 - g. l'inserimento di segnalibri (bookmark virtuali) nelle registrazioni, per evidenziare un determinato Evento e poter in seguito individuarlo più facilmente sui file di sistema, senza avere impatto sulla durata di conservazione delle Registrazioni (restano applicabili le durate ordinarie di conservazione delle stesse);
 - h. l'utilizzo di un'apposita funzione per la conservazione di mezzi di prova;
 - i. la conservazione e/o l'esportazione delle Registrazioni dal sistema di videosorveglianza tramite l'apposita funzione di conservazione di mezzi di prova.
- ⁵ Si applica il principio del minimo privilegio, ossia l'attribuzione al Personale autorizzato che ricopre i ruoli definiti dall'**Allegato 2** unicamente dei diritti e degli accessi strettamente necessari allo svolgimento delle mansioni assegnate.

Art. 9
Visualizzazione di
Riprese live e/o
Playback a fini
operativi

- ¹ Salvo quanto diversamente previsto nelle presenti Disposizioni e nell'**Allegato 2**, la visualizzazione da parte del Personale autorizzato delle Riprese live o, se del caso, del Playback, per assicurare la sicurezza e/o la logistica presso le Sedi universitarie, avviene alle seguenti condizioni minime e finalit :
 - a. previa autorizzazione nominativa, ai sensi dell'**Allegato 2**;
-

-
- b. solo se giustificata da un Evento, verificatosi o segnalato nell'ambito dell'attività di sorveglianza, in seguito documentato e portato all'attenzione dello Specialista salute e sicurezza;
 - c. di principio solo con filtri e maschere privacy attivi. È richiesta un'autorizzazione specifica, definita di default, secondo quanto previsto all'**Allegato 2**, per rimuovere le maschere rimovibili, in caso di necessità operative basate sugli obiettivi di sicurezza, opportunamente documentate;
 - d. limitatamente alla durata del turno di servizio, al cui termine il membro del Personale autorizzato interessato è tenuto a disconnettersi; e
 - e. in caso di visualizzazione del Playback, unicamente per verificare circostanze sospette antecedenti riconducibili ad un Evento e, se del caso, procedere alla relativa segnalazione.
- ² Le autorizzazioni di cui al cpv. 1 sono gestite come privilegi speciali impostati di default con obbligo di protocollazione all'interno del sistema di gestione della videosorveglianza, secondo quanto previsto all'**Allegato 2**, in particolare per i ruoli incaricati della sorveglianza/sicurezza nonché per tutto o parte delle Guardianie. Ulteriori autorizzazioni possono essere rilasciate dalla Direzione, a titolo eccezionale e in forma scritta. Esse devono essere protocollate, rendicontate ed essere limitate nel tempo.
- ³ Il collegamento al sistema di videosorveglianza dell'USI da remoto e/o tramite dispositivi mobili di servizio è eccezionalmente consentito ai soli membri del Personale espressamente autorizzati, nei ruoli e nei casi di cui all'**Allegato 2**, alle seguenti condizioni aggiuntive:
- a. utilizzo di connessioni sicure e crittografate (connessioni HTTPS; VPN; autenticazione a doppio fattore "MFA");
 - b. il dispositivo utilizzato deve essere conservato e configurato in modo da garantire la sicurezza delle applicazioni e dei dati trattati, nonché la disponibilità dello stesso a beneficio degli altri membri del Personale autorizzato;
 - c. al termine del rispettivo turno, il membro del Personale autorizzato interessato è imperativamente tenuto a terminare la sessione, disconnettendosi.
- ⁴ Le Guardianie permettono di principio la visualizzazione delle Riprese live in chiaro delle aree sorvegliate da una postazione fissa, di regola senza possibilità di Playback, fatti salvi i casi previsti nell'**Allegato 2**. In tale contesto, vanno osservate le seguenti regole:
- a. la visualizzazione delle Riprese live è limitata alla sola durata del tempo di apertura della Sede universitaria sorvegliata;
 - b. il Personale autorizzato è tenuto a disconnettersi dal proprio account personale con il quale è, se del caso, collegato e/o a spegnere gli schermi al termine del turno o dell'orario di apertura della Sede universitaria sorvegliata.
- ⁵ La visualizzazione delle Riprese live e, se del caso, del Playback, è parimenti consentita eccezionalmente alle autorità preposte o alle forze dell'ordine, su loro richiesta, in casi eccezionali e urgenti, segnatamente un'emergenza che coinvolge beni giuridici di primaria importanza, alle condizioni di legge, e dopo essere stata approvata dalla Direzione. In caso non fosse possibile ottenere tempestivamente l'autorizzazione di tutti i membri della Direzione, l'approvazione può essere concessa anche solo da un membro della Direzione, che informa quanto prima i restanti membri.
-

Art. 10
Accesso operativo
alle Registrazioni -
Motivi e
legittimazione

- ¹ Senza pregiudizio per quanto previsto all'art. 9 delle presenti Disposizioni, l'accesso diretto alle Registrazioni a fini operativi è esclusivamente consentito in uno dei casi seguenti:
- a. in presenza di un ordine di perquisizione e/o sequestro o di atti giuridici equivalenti notificati da parte di autorità giudiziarie penali, civili o amministrative, per prepararne la Trasmissione;
 - b. in caso di comprovata esigenza dell'USI di disporre di mezzi di prova nell'ambito di procedure civili, penali o amministrative relative a reati commessi contro i propri collaboratori, contro le infrastrutture dell'Università (da intendersi sia di proprietà che gestite/utilizzate nell'ambito della responsabilità di USI), o contro utenti terzi tutelati ai sensi delle finalità esposte nel Regolamento, oppure per difendere i propri legittimi interessi in qualsiasi tipo di procedura indirizzata contro l'Università o contro i suoi collaboratori in relazione allo svolgimento di attività correlata al rapporto di impiego;
 - c. in caso di comprovata situazione di emergenza, che coinvolge beni giuridici di primaria importanza, alle condizioni di legge.
- ² L'accesso diretto alle pertinenti Registrazioni è concesso di principio unicamente allo Specialista salute e sicurezza, e se del caso eccezionalmente alla Direzione nei casi previsti al precedente cpv. 1 lett. b-c.
- ³ Gli utenti delle Sedi universitarie, i collaboratori, gli studenti, gli organi, i fornitori, i mandatarî, i proprietari o terze parti al di fuori di quelle persone debitamente autorizzate e aventi i ruoli previsti dall'**Allegato 2** alle presenti Disposizioni, non hanno in alcun caso diritto di richiedere e/o ottenere alcun tipo di accesso alle Registrazioni della videosorveglianza. Essi devono rivolgersi alle autorità giudiziarie competenti.

Art. 11
Accesso operativo
alle Registrazioni -
Procedura per la
gestione di
segnalazioni di
Eventi o richieste
di Trasmissione

- ¹ Ogni segnalazione – interna o esterna – di un Evento che implica potenzialmente l'accesso alle Registrazioni viene di principio gestita come segue:
- a. il Responsabile interno, per il tramite dello Specialista salute e sicurezza:
 - i. prende personalmente a carico la segnalazione, nonché la documentazione di supporto, analizzando la segnalazione e se del caso l'eventuale richiesta di Trasmissione, e istruendo un dossier interno;
 - ii. provvede a selezionare le Registrazioni pertinenti in termini di tempo e luogo e attiva cautelativamente la funzione di conservazione di mezzi di prova, in particolare per evitare la cancellazione automatica delle Registrazioni (cfr. art. 12 cpv. 3);
 - iii. qualora la segnalazione sia legata ad una richiesta di Trasmissione:
 - valuta la legittimità della richiesta, coadiuvato se del caso dal CPD e dal SLC; verifica in particolare la presenza di un ordine formale in originale emesso da parte di un'autorità competente penale, civile o amministrativa nell'ambito di un procedimento pendente;
 - provvede, nei casi ritenuti legittimi, a informare quanto prima la Direzione, il CPD e il SLC, fornendo tutti i principali elementi del dossier aperto. In tutti gli altri casi, rinvia la persona richiedente a rivolgersi alle competenti autorità, senza fornire ulteriori informazioni;
 - raccoglie da parte della Direzione le necessarie autorizzazioni ai sensi degli art. 12 e 13 e – in caso positivo – provvede a dare seguito alla richiesta;

-
- iv. qualora invece una segnalazione implichi un accesso della Direzione ai sensi dell'art. 10 cpv. 1 lett. b-c delle presenti Disposizioni, in particolare per valutare gli estremi per una denuncia o simile atto introduttivo di una procedura penale, civile o amministrativa, esegue la richiesta tenuto conto dei principi e dell'insieme delle norme applicabili, alla luce del motivo d'accesso invocato, coadiuvato se del caso dal CPD e dal SLC;
 - v. redige e conserva i necessari protocolli relativi al dossier.
- ² Eventuali deroghe alla procedura descritta in precedenza sono eccezionalmente ammesse in casi gravi e urgenti, in particolare nel caso in cui l'USI debba agire tempestivamente per tutelare beni giuridici di particolare rilievo. In tale contesto, la Direzione può, eccezionalmente e limitatamente per la durata dell'emergenza:
- a. richiedere di visionare una o più Registrazioni della videosorveglianza;
 - b. dare accesso alle competenti forze dell'ordine od autorità, sottostanti alle proprie normative specifiche, alle Riprese live (art. 9 cpv. 5) e/o alle Registrazioni (art. 10 cpv. 1 lett. c), in modo sicuro e crittografato.
- ³ Entro 24 ore dalla conclusione dell'emergenza deve essere steso un protocollo che adempia i requisiti espressi all'art. 14 delle presenti Disposizioni.
-

Art. 12
Conservazione e
cancellazione delle
registrazioni

- ¹ In conformità con il quadro giuridico applicabile, le Registrazioni della videosorveglianza sono conservate per la durata prevista all'art. 6 del Regolamento.
- ² Decorso il periodo di conservazione, le Registrazioni della videosorveglianza vengono cancellate in modo automatico e definitivo dal sistema di gestione della videosorveglianza, tramite cancellazione logica dei dati, affiancata dalle opportune misure tecniche e organizzative atte a impedire l'accesso non autorizzato ai supporti fisici di memorizzazione degli stessi.
- ³ In caso di verosimile o certa esigenza di conservazione di Registrazioni, dettata segnatamente da una segnalazione interna o esterna di un Evento, il Responsabile interno, tramite lo Specialista salute e sicurezza di cui all'**Allegato 2**, provvede:
- a. Senza attendere, entro il termine di conservazione previsto, a salvare copia delle specifiche Registrazioni rilevanti tramite apposita funzione di conservazione di mezzi di prova, per esigenze investigative e probatorie (cfr. art. 11 cpv. 1 lett. a.ii);
 - b. Senza attendere, a richiedere alla Direzione l'autorizzazione scritta all'ulteriore conservazione di tale copia oltre la durata prevista dal Regolamento.
- ⁴ La Direzione, supportata dal CPD e, in caso di necessità, dal SLC, conferma quanto prima, con provvedimento motivato e scritto, la conservazione ulteriore della copia di specifiche Registrazioni, nei seguenti casi:
- a. In caso di una procedura civile, amministrativa o penale – anche nel caso in cui non sia stata ancora notificata una richiesta di Trasmissione nell'ambito della fattispecie di cui all'art. 10 cpv. 1 lett. a, per la durata della stessa; al termine di cui la copia deve essere irreversibilmente distrutta (art. 6 cpv. 3 Regolamento);
 - b. Nei casi di cui all'art. 6 cpv. 2 del Regolamento e all'art. 10 cpv. 1 lett. b e c delle presenti Disposizioni, per il tempo necessario a valutare se le
-

pertinenti Registrazioni sono necessarie per la tutela dei diritti menzionati o fino a ricezione di una richiesta ai sensi dell'art. 10 cpv. 1 lett. a.

- ⁵ Fatta salva l'apertura di una procedura (cfr. art. 12 cpv. 4 lett. a) o l'adozione di una specifica decisione di proroga della Direzione debitamente motivata, il termine di conservazione di specifici mezzi di prova non può eccedere 360 giorni dall'inserimento della funzione di conservazione dei mezzi di prova.
- ⁶ In assenza di una conferma specifica da parte della Direzione ai sensi del cpv. 4, il Responsabile interno, tramite lo Specialista salute e sicurezza, provvede – se del caso dopo sollecito – a cancellare senza indebito ritardo le Registrazioni salvate.

Art. 13
Esportazione e
trasmissione delle
Registrazioni a
terzi

- ¹ L'esportazione e successiva Trasmissione di specifiche Registrazioni è permessa solo al Personale autorizzato ai sensi dell'**Allegato 2**, in favore delle autorità giudiziarie o amministrative competenti di cui all'art. 7 cpv. 2 del Regolamento. Essa deve essere previamente confermata per iscritto dalla Direzione.
- ² Il Personale autorizzato di cui all'**Allegato 2**, per eseguire l'esportazione, accede alle Registrazioni proporzionalmente e se possibile in modo indiretto (che non implica di regola una visualizzazione dei filmati), esportando solo quelle Registrazioni riferite ad un determinato lasso temporale e relative ad un'area ben definita delle Sedi universitarie pertinenti.
- ³ In caso di esportazione e Trasmissione delle Registrazioni nell'ambito dell'art. 7 cpv. 2 del Regolamento, la documentazione relativa all'introduzione della relativa procedura e/o all'espletamento di una richiesta ai sensi dell'art. 10 cpv. 1 lett. a delle presenti Disposizioni deve essere allegata ad un protocollo di esportazione, unitamente alla conferma scritta della Direzione, e mantenuta per 10 anni riservate particolari esigenze probatorie o le disposizioni della Legge cantonale sull'archiviazione e sugli archivi pubblici (LArch).
- ⁴ La Trasmissione delle Registrazioni deve avvenire in modo confidenziale e sicuro, utilizzando metodi di comunicazione crittografati secondo le migliori pratiche di sicurezza dell'informazioni applicabili in USI. Le credenziali di decodifica dei file esportati (password) devono essere condivise separatamente, utilizzando canali sicuri.
- ⁵ Ogni comunicazione deve essere destinata a persone fisiche identificate o identificabili interne al destinatario definito e autorizzato (ad es. Sig. Rossi o Procuratore pubblico).

Art. 14
Protocolloazione,
tracciabilità e
registri di audit

- ¹ Fatto salvo quanto segue, ogni accesso alle Registrazioni della videosorveglianza deve essere dettagliatamente protocollato, includendo le seguenti informazioni:
 - a. la data e l'orario dell'accesso;
 - b. il motivo dell'accesso/Evento;
 - c. l'identità del membro del Personale autorizzato operante;
 - d. le videocamere o le aree delle Sedi universitarie visualizzate;
 - e. l'intervallo temporale esaminato o esportato.
 - ² In caso di esportazione delle Registrazioni a seguito, segnatamente, di una richiesta legittima, sono inoltre protocollati:
-

	a. i motivi della richiesta, rispettivamente l'esigenza di Trasmissione; b. i destinatari della Trasmissione; c. le misure di protezione della confidenzialità adottate. ³ Qualora il sistema informativo non preveda la tracciabilità automatica di tutte o parte delle informazioni di cui ai capoversi precedenti, il Responsabile interno è responsabile per la tenuta delle informazioni mancanti tramite un sistema di registrazione delle informazioni manuale da affiancare alle informazioni e ai dati automaticamente protocollati e/o registrati dal sistema di videosorveglianza. ⁴ Il sistema registra le attività svolte (log), per garantire la tracciabilità di quanto fatto dai singoli membri del Personale autorizzato, e l'attribuzione delle responsabilità in caso di bisogno. ⁵ Vigono inoltre i seguenti criteri di protocollazione: a. La visualizzazione o l'accesso alle Registrazioni della videosorveglianza, senza filtri, maschere privacy o altro (fatto salvo il caso delle Guardianie specificatamente autorizzate per default) deve essere espressamente e specialmente protocollato con l'indicazione dei motivi; b. l'accesso indiretto alle registrazioni per le esigenze operative autorizzate può limitarsi ad una sommaria descrizione dei motivi dell'accesso, con indicazione di area, tempo e durata di eventuali Registrazioni esportate. ⁶ Eventuali incidenti (segnatamente, violazioni di sicurezza, perdita di dati, smarrimento dei dispositivi mobili di accesso e/o accessi non autorizzati) devono essere protocollati il prima possibile indicando, in particolare, data, ora, componenti dell'impianto coinvolte, descrizione delle circostanze, e notificati al CPD entro 12 ore dalla loro redazione secondo i canali previsti. ⁷ I log di sistema e di attività sono conservati per un periodo massimo di 1 anno, conformemente alle esigenze operative, di sicurezza e regolamentari. Essi possono essere verificati puntualmente per identificare eventuali violazioni. ⁸ Il Responsabile interno, coadiuvato dall'Amministratore di sistema, è responsabile per l'attuazione, definizione e configurazione dei sistemi e delle misure per la raccolta e conservazione dei log, nonché dei processi di gestione degli stessi, sotto il profilo tecnico e organizzativo.
Art. 15 Deroghe	Le Registrazioni della videosorveglianza devono essere utilizzate esclusivamente per gli scopi definiti nel Regolamento, nelle presenti Disposizioni e conformemente alle procedure approvate. Eventuali deroghe sono ammesse unicamente in via eccezionale, quale un'estrema urgenza per la sicurezza di beni giuridici importanti, previa approvazione scritta della Direzione. In caso non fosse possibile ottenere tempestivamente l'autorizzazione di tutti i membri della Direzione, l'approvazione può essere concessa anche solo da un membro della Direzione, che informa quanto prima i restanti membri.
Art. 16 Nuovi impianti, sostituzione, modifica e/o dismissione degli impianti di videosorveglianza	¹ Il Responsabile interno è l'unica figura autorizzata a gestire, con il necessario supporto della Direzione, dell'Amministratore di sistema, del CPD, l'installazione di nuovi impianti di videosorveglianza. A tal fine, esso predispone e sottopone, con il supporto del CPD e dell'Amministratore di sistema, una specifica richiesta documentata all'attenzione della Direzione. ² Ai fini della richiesta di cui al cpv. 1, il Responsabile interno documenta per iscritto il trattamento prospettato, indicando in particolare le finalità, la tipologia di impianto e il luogo di installazione, e formula un parere tecnico.

In tale parere si esprime segnatamente in merito alla fattibilità e alla sostenibilità dell'installazione, nonché alla scelta della strumentazione tecnologica più idonea in funzione delle finalità indicate e delle specifiche tecniche richieste, alla luce delle direttive interne di sicurezza dell'USI.

- ³ In caso di valutazione positiva da parte della Direzione, il Responsabile interno provvede all'implementazione del nuovo impianto di videosorveglianza conformemente al Regolamento, alle Disposizioni, e alle indicazioni ricevute, assumendosene la responsabilità, e redige un apposito verbale in merito alle operazioni eseguite.
- ⁴ Qualora la scelta tecnologica o il tipo di impianto sottoposto al vaglio della Direzione dell'USI presenti elementi di criticità dal punto di vista della protezione dei dati personali, il Responsabile interno informa il CPD in merito ai punti di attenzione rilevati e richiede allo stesso un parere sulla conformità del trattamento alla normativa applicabile in materia di protezione dati. L'analisi del CPD deve essere inclusa nel parere tecnico di cui al cpv. 2.
- ⁵ La sostituzione di singole videocamere in caso di malfunzionamento non costituisce una modifica o potenziamento del sistema di videosorveglianza esistente, a condizione che la configurazione delle nuove videocamere corrisponda a quella precedentemente autorizzata. Il Responsabile interno documenta la sostituzione in modo adeguato.
- ⁶ La modifica del sistema di videosorveglianza (segnatamente a seguito di un aggiornamento di eventuali software con implicazioni per i diritti e le libertà degli utenti delle Sedi universitarie) è parificata ad una nuova installazione. Il Responsabile interno istruisce la pratica per verificare la conformità delle installazioni e delle modifiche proposte, effettua sopralluoghi, relaziona per iscritto alla Direzione e fornisce le planimetrie con indicazione della scala utilizzata nella rappresentazione del diagramma o progetto. Il Responsabile interno aggiorna inoltre la documentazione necessaria nei casi di modifica e dismissione degli impianti.

Art. 17
Violazioni delle
prescrizioni
applicabili

- ¹ In generale, sono vietati comportamenti idonei a compromettere la strategia di sicurezza o le finalità legittime del sistema di videosorveglianza dell'USI, e in particolare:
 - a. La visualizzazione o l'accesso non autorizzato alle Registrazioni della videosorveglianza;
 - b. l'utilizzo di strumenti informatici privati e/o l'installazione non autorizzata di software che consenta, anche potenzialmente, la visualizzazione delle riprese delle videocamere in tempo reale e/o l'accesso alle registrazioni in modo non autorizzato;
 - c. il collegamento al sistema di videosorveglianza da postazioni non autorizzate (cfr. **Allegato 2**);
 - d. la visione di registrazioni o flussi live senza uno scopo specifico, legittimo, e documentato, segnatamente al fine di effettuare ricerche generiche di infrazioni commesse nelle Sedi universitarie;
 - e. l'utilizzo di credenziali condivise. Fanno eccezione le Guardianie che, ai sensi dell'**Allegato 2** e dell'art. 8 cpv. 2 delle presenti Disposizioni, utilizzano postazioni fisse autorizzate e configurate dal Responsabile interno e dall'Amministratore di sistema.
 - ² La violazione dei precitati doveri e oneri, come anche delle procedure vincolanti e degli ulteriori obblighi di cui al Regolamento e alle presenti Disposizioni, può costituire una violazione degli obblighi del Personale
-

	autorizzato e comportare l'adozione di adeguati provvedimenti da parte del Titolare dell'elaborazione secondo i regolamenti vigenti e gli accordi in essere. ³ La Direzione, avvalendosi dei competenti servizi, al fine di accertare sospette violazioni del Regolamento e delle presenti Disposizioni, può trattare log e altre informazioni connesse alla gestione della videosorveglianza. Valgono a questo riguardo i seguenti criteri: a. La violazione di norme comportamentali sull'uso delle risorse informatiche, o il relativo sospetto, va constatato di principio tramite una sorveglianza non nominativa dei dati raccolti, o grazie ad indizi fortuiti. b. È tuttavia ammessa l'analisi nominativa puntuale dei dati personali raccolti tramite sistemi di sorveglianza, in caso di constatazione o di relativi sospetti concreti di violazione delle norme comportamentali di cui al Regolamento e alle presenti Disposizioni. ⁴ Per quanto non espressamente previsto dalle presenti Disposizioni, si applicano i regolamenti e le direttive interne dell'USI, nonché la normativa vigente, in particolare in relazione al rapporto di collaborazione con il Personale autorizzato.
Art. 18 Revisione e aggiornamento	¹ La conformità delle presenti Disposizioni e la loro attuazione sono oggetto di verifiche periodiche e, laddove opportuno, esse sono sottoposte a revisione per garantire il rispetto delle normative applicabili e delle direttive interne dell'Università. ² La revisione periodica include, in particolare, il controllo: a. delle configurazioni dei ruoli e dei privilegi attribuiti al Personale autorizzato nel software di riferimento; b. della corretta configurazione e conservazione dei registri di audit; c. dell'applicazione delle misure tecniche previste, tra cui la crittografia e il mascheramento delle riprese, per assicurare l'allineamento con le normative applicabili. ³ Il Responsabile interno definisce e attua le opportune misure organizzative e operative necessarie per dare esecuzione a quanto previsto al presente art. 18.
Art. 19 Videosorveglianza per conto di terzi	¹ In caso di stipulazione di accordi e/o di conferimento di responsabilità da parte di altri titolari del trattamento, ai sensi e nei limiti di cui all'art. 9 del Regolamento, possono prevalere specifiche disposizioni e impegni contrattuali, a patto che tali accordi non contraddicano la legge applicabile e il Regolamento, e non pregiudichino i processi operativi interni e le risorse dell'Università. ² In particolare, salvo specifici accordi, eventuali titolari del trattamento rimangono di principio responsabili giuridicamente per fornire un'adeguata informazione ai soggetti interessati, e per evadere richieste di esercizio di eventuali diritti in materia di protezione dei dati. ³ Per quanto riguarda le competenze decisionali in caso di necessità, gli accordi possono prevedere la competenza di un organo differente rispetto alla Direzione, assumendosi tuttavia il titolare del trattamento la piena responsabilità.
Art. 20 Entrata in vigore	Le presenti Disposizioni vengono approvate in data 24 agosto 2026 ed entrano in vigore con effetto immediato.

Allegato 1 – Sedi universitarie

Sedi *	Stabili e aree oggetto della videosorveglianza
Campus di Lugano Ovest (LUO), Via Giuseppe Buffi 13, 6900 Lugano	Palazzo principale (e spazi esterni)
	Aula magna
	Palazzo nero
	Palazzo rosso
	Stabile Lab
	Biblioteca universitaria Lugano
	Stabile Facoltà di Teologia
	Palazzo blu
Campus di Lugano Est (LUE), Via alla Santa 1, 6962 Lugano-Viganello	Stabile Campus Est Lugano (e piazzale interno)
Campus di Mendrisio (ME), Largo Maria Bernasconi 2, 6850 Mendrisio	Palazzo Turconi
	Palazzo Canavée
	Teatro dell'architettura Mendrisio (TAM)
Guardianie	Ricezione Palestra LUE (PLUE)
	Ricezione ME (RiME)
	Plotter ME (PlOME)
	Ricezione TAM

* cfr. lista stabili completa su: <https://www.usi.ch/it/universita/dove-siamo>

Allegato 2 - Ruoli e privilegi

Ruolo operativo	Funzione in USI	Luogo di competenza	Posizione lavorativa autorizzata			Privilegi Videosorveglianza								
			Fissa	PC personale	Cellulare di servizio	Riprese live		Playback ¹		Registrazioni		Segnalibri	Evidence Lock	Cellulare
						Blur	Chiaro	Blur	Chiaro	Blur	Chiaro			
Cellula di crisi²	Direzione	Tutte le Sedi	LUO	LUO, LUE, ME, remoto	No	1	1	1	1	1	1	1	1	1
Specialista salute e sicurezza	Specialista salute e sicurezza	Tutte le Sedi	LUO	LUO, LUE, ME, remoto	No	0	0	0	0	1	1	1	1	0
(Sostituto)	Responsabile Servizio logistica e sicurezza	Tutte le Sedi	LUO	LUO, LUE, ME, remoto	No	0	0	0	0	1	1	1	1	0
Supporto occasionale diurno-feriale	Specialista salute e sicurezza	Tutte le Sedi	LUO	LUO, LUE, ME, remoto	No	1	1	1	1	0	0	1	0	0
Sostituto (LU)	Coordinatore logistica LU	LUO e LUE	LUO	No	No	1	0	1	0	0	0	1	0	0
Sostituto (ME)	Coordinatore logistica ME	ME	ME	No	No	1	0	1	0	0	0	1	0	0
Sorveglianza notturna e festivi														
Sorvegliante interno LU	Collaboratori sorveglianza	LUO e LUE	LUO	No	LUO, LUE, remoto	1	1	1	1	0	0	1	0	1
Sorvegliante esterno LU	Mandatari esterni	LUO e LUE	LUO	No	LUO, LUE, remoto	1	1	1	1	0	0	1	0	1
Sorvegliante esterno ME	Mandatari esterni	ME	ME	No	ME, remoto	1	1	1	1	0	0	1	0	1
Responsabile Guardiania PLUE^{3 4}	Responsabile Servizio sport	Palestra LUE	PLUE	No	No	1	1	1	1	0	0	1	0	0
(Co-responsabile)	Coordinatore Servizio SPORT	Palestra LUE	PLUE	No	No	1	1	1	1	0	0	1	0	0

Responsabile Guardiania RiMe⁵	Coordinatore Servizio Ricezione-alloggi ME	Posteggi ME	RiME	No	No	0	1	0	0	0	0	0	0	0
(Sostituti)	Collaboratori Servizio Ricezione-alloggi ME	Posteggi ME	RiME	No	No	0	1	0	0	0	0	0	0	0
Guardiania TAM⁶	Responsabile Teatro dell'architettura Mendrisio	TAM	TAM	No	No	0	1	0	0	0	0	0	0	0
	Collaboratori/saltuari Teatro dell'architettura Mendrisio	TAM	TAM	No	No	0	1	0	0	0	0	0	0	0
Responsabile Guardiania PloME	Coordinatore Servizio IT - Help desk	ME	PloME	No	No	0	1	0	0	0	0	0	0	0
(sostituto)	Collaboratore Servizio IT - help desk	ME	PloME	No	No	0	1	0	0	0	0	0	0	0
Admin IT⁷	Collaboratore Servizio IT - Sistemi e reti	Tutte le Sedi	LUO	LUO, LUE, ME, remoto	No	1	1	0	0	0	0	0	0	0
(Sostituto)	Collaboratore Servizio IT - Sistemi e reti	Tutte le Sedi	LUO	LUO, LUE, ME, remoto	No	1	1	0	0	0	0	0	0	0
Admin sicurezza IT	Collaboratore Servizio IT - Sistemi e reti	Tutte le Sedi	LUO	LUO, LUE, ME, remoto	No	0	0	0	0	0	0	0	0	0

¹ Salvo per Guardiania PLUE, Playback permesso per un massimo di 6h.

² Su attivazione, secondo le normative e i processi vigenti in USI in caso di emergenza.

³ Playback permesso per un massimo di 12h.

⁴ Live permesso tra le 10-20h00 dei giorni feriali.

⁵ Live permesso tra le 8h30-17h00 dei giorni feriali.

⁶ Live permesso tra le 10-18h00, e in caso di aperture straordinarie.

⁷ Accesso permesso solo nell'ambito della configurazione delle telecamere.