ACCORDO SULL'UTILIZZO DEI METADATI E DEI LOG EX ARTICOLO 4 DELLA LEGGE 300/70 (STATUTO DEI LAVORATORI)

Il giorno 19 dicembre 2025 presso l'Università degli Studi di Milano si riuniscono la Delegazione di Parte Pubblica e la Delegazione di Parte Sindacale;

PREMESSO CHE l'Università degli Studi di Milano è tenuta, anche in ottemperanza a norme di legge recentemente entrate in vigore, ad assicurare la tutela del suo patrimonio digitale e la sicurezza informatica, mediante sistemi di cybersicurezza, nel rispetto dei diritti e delle libertà fondamentali delle persone interessate, con particolare riferimento alla riservatezza e all'identità personale, e nel pieno rispetto dei principi di liceità, necessità e proporzionalità;

VISTA la Legge 20 maggio 1970, n. 300, recante Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento, (di seguito Statuto dei Lavoratori), e in particolare l'art. 4 (Impianti audiovisivi e altri strumenti di controllo), che dispone: "1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi. 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. 3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.";

VISTO il Regolamento europeo in materia di protezione dei dati personali (di seguito, Regolamento UE 2016/679 o "RGPD") e l'art. 88, in particolare, che individua tassativamente le finalità (ovvero quelle organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale) per le quali gli **strumenti,** dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere impiegati nel contesto lavorativo, prevedendo garanzie procedurali (accordo sindacale o autorizzazione pubblica, ex art. 114 del Codice, che richiama l'art. 4, c. 1, dello Statuto dei Lavoratori, come modificato dal D. Lgs. 151/2015).;

VISTO il d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) e in particolare l'art. 114 recante "Garanzie in materia di

controllo a distanza", in base al quale resta fermo quanto disposto dall'articolo 4 della Legge 20 maggio 1970 n. 300;

VISTO il d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) e in particolare le disposizioni in materia di sicurezza informatica e sull'utilizzo di servizi e strumenti infotelematici;

VISTE le Linee Guida per posta elettronica e internet, del Garante della privacy, deliberazione n. 13 del 10 marzo 2007, pubblicata sulla G.U. n. 58 del 10 marzo 2007;

VISTO il provvedimento del Garante per la protezione dei dati personali n. 364 del 6 giugno 2024 "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", che fornisce nuove indicazioni sul trattamento dei metadati della posta elettronica e sui tempi di conservazione, precisando che la raccolta dei metadati per un lasso di tempo più esteso di 21 giorni, anche per finalità di sicurezza informatica e tutela del patrimonio, comporta un controllo a distanza dei lavoratori e richiede l'esperimento delle garanzie previste dal comma 1 dell'art. 4 dello Statuto dei lavoratori;

RICORDATO che in esecuzione del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", l'Ateneo ha provveduto all'individuazione e alla nomina dei soggetti incaricati dello svolgimento di mansioni di "amministratori di sistema", anche in relazione alla gestione e al monitoraggio dei sistemi informativi e delle reti dell'Ateneo che utilizzano log e metadati, secondo criteri di esperienza, capacità e affidabilità;

VISTO il Decreto-Legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla Legge 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza", che ha definito l'architettura nazionale della cybersicurezza e istituito l'Agenzia per la cybersicurezza nazionale (ACN) con l'obiettivo di pubblicare dati e documenti relativi ai servizi, alla struttura e alle attività svolte da ACN e di fornire a pubbliche amministrazioni, imprese e cittadini informazioni sul settore di competenza;

VISTA la Direttiva (UE) 2555/2022 [NIS2], come recepita dal D.Lgs. 4 settembre 2024, n.138, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, che ha aggiornato e sostituito la precedente Direttiva NIS (Direttiva (UE) 1148/2016, stabilendo standard elevati di sicurezza informatica all'interno dell'Unione Europea a protezione delle infrastrutture critiche e del miglioramento della resilienza delle reti e dei sistemi informativi essenziali per la società e l'economia. La Direttiva NIS2 ha esteso l'elenco dei settori considerati critici dal punto di vista della sicurezza informatica, includendo nuove categorie di operatori;

TENUTO CONTO che con Determinazione del Direttore generale dell'ACN n. 63819 del 25 febbraio 2025 l'Università degli Studi di Milano è stata individuata per le finalità dalla predetta legge in qualità di "Soggetto Importante" tenuto, tra gli altri obblighi, all'adozione di misure di sicurezza specifiche per la gestione di rischi informatici che includono anche la gestione della sicurezza della catena di approvvigionamento (supply chain), la sicurezza delle comunicazioni, la gestione delle vulnerabilità e la formazione dei/delle dipendenti;

VISTE le "Linee guida per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio" pubblicate a novembre 2024 dall'Agenzia per la cybersicurezza nazionale (ACN),

le quali prevedono che le politiche di sicurezza adottate per la gestione dei log esistenti, con particolare riguardo all'integrità e alla disponibilità dei log, devono prevedere la loro conservazione in modo sicuro, possibilmente centralizzato, per almeno 24 mesi;

VISTO il Codice di comportamento dei/delle dipendenti pubblici, a norma dell'articolo 54 del d.lgs. 30 marzo 2001, n. 165, approvato con il d.P.R. 16 aprile 2013, n. 62, e modificato con il d.P.R. 13 giugno 2023, n. 81, e in particolare l'art. 11 bis che dispone in materia di utilizzo delle tecnologie informatiche, prevedendo, tra l'altro, che l'Amministrazione, attraverso i/le propri/e responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati e che le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali, ad oggi ancora non adottate;

VISTO il Codice di comportamento per il personale dell'Università degli Studi, emanato con D.R. n. 295200, l'8 maggio 2015, e in particolare l'art. 10 - Comportamento in servizio, che disciplina tra l'altro i doveri del personale nell'utilizzo e custodia degli strumenti e servizi infotelematici;

DATO ATTO che l'Ateneo per il perseguimento dei propri compiti istituzionali

- fornisce al proprio personale strumenti e servizi ICT, considerando anche il ruolo ricoperto nell'organizzazione e necessari per lo svolgimento delle proprie funzioni, in particolare la postazione di lavoro (di seguito PdL), l'account Microsoft che include la casella di posta elettronica nominativa da utilizzare alle condizioni e nei limiti stabiliti dai regolamenti adottati dall'Ateneo, l'antivirus, il software per la produttività individuale e l'accesso alla rete pubblica e privata (intranet);

- gestisce quanto sopra indicato, talvolta, anche tramite contratti con operatori economici qualificati esterni e nominati responsabili del trattamento ai sensi dell'art. 28 del RGPD;

- questi strumenti e servizi producono, anche automaticamente, log tecnici e di sicurezza, sia per tenere sotto controllo il loro funzionamento sia per tutelare il patrimonio digitale e rispettare la normativa;

DATO ATTO che

- l'uso degli strumenti e servizi ICT è consentito secondo quanto previsto dalle richiamate disposizioni di legge e del Codice di comportamento;

- l'utilizzo dei suddetti strumenti e servizi ICT, obbligatorio e indispensabile, espone il patrimonio digitale dell'Ateneo e le sue attività a rischi di compromissione dell'integrità, confidenzialità e disponibilità dei dati personali e del patrimonio digitale stesso, in ragione dei quali è doverosa la messa in campo di azioni e interventi di presidio della sicurezza informatica e alla protezione del dato;

- l'Ateneo per:

a) garantire il funzionamento e la continuità operativa dei sistemi e dei servizi ICT;
b) verificare la funzionalità dei sistemi informativi, delle reti dell'Ateneo;
c) gestire il ciclo di vita dei dispositivi e degli asset forniti;

d) tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
e) evitare che siano reiterati illeciti o per esigenze di carattere difensivo;
f) gestire gli incidenti informatici;
g) analizzare le possibili anomalie e le relative cause, a tutela del patrimonio digitale dell'Ateneo;

ha avviato un processo strutturato per l'adozione di politiche e l'aggiornamento delle regolamentazioni relative alla sicurezza informatica e all'utilizzo di strumenti e servizi ICT. Queste procedure mirano a garantire la sicurezza, l'efficienza operativa dei sistemi informativi e delle reti, nonché la protezione e la riservatezza dei dati. Sono inoltre previste attività di monitoraggio e controllo dei metadati e dei log tecnici generati automaticamente dagli strumenti o servizi impiegati.

Le suddette disposizioni rientrano nelle prerogative istituzionali dell'Ateneo e non costituiscono oggetto del presente Accordo; potranno essere soggette a modifiche in base ad eventuali nuove esigenze organizzative, previo tempestivo avviso alle OO.SS. e successiva diffusione delle informazioni rilevanti a tutto il personale.

CONSIDERATO altresì che

- per le suddette finalità e in ragione delle caratteristiche non modificabili degli strumenti e dei servizi ICT, l'Ateneo ha necessità di conservare i relativi log e metadati per un periodo superiore a 21 giorni ma non oltre i tempi di conservazione previsti nel dettaglio nel prosieguo del presente accordo (da 90 gg a 24 mesi, in base alla tipologia di servizio)e quindi per un tempo superiore a quello indicato dal Garante per la protezione dei dati personali nel sopracitato provvedimento n. 364/2024;

- i log sono registrazioni tecniche che documentano le interazioni di un sistema, come i log di navigazione web (siti visitati) o i log di trasporto delle email (inclusi dati come indirizzi IP, orari, dimensioni dei messaggi).

- i metadati, nel contesto del provvedimento del Garante, sono le informazioni strutturate contenute nei log, che descrivono altri dati senza rivelare il contenuto effettivo (ad esempio, mittente, destinatario e orari di invio delle email, non il loro corpo)

- tali log/metadati possono configurarsi come dati personali riguardanti lavoratori/trici, identificati/e o identificabili;

VISTO che il Collegio dei Revisori dei Conti, nella seduta del 15 dicembre 2025, ha preso atto dell'Ipotesi di Accordo sull'utilizzo dei metadati e dei log ex articolo 4 della legge 300/70;

CONSIDERATO che il Consiglio di Amministrazione, in data 16 dicembre 2025, ha autorizzato alla sottoscrizione in via definitiva dell'Ipotesi di Accordo sull'utilizzo dei metadati e dei log ex articolo 4 della legge 300/70, sottoscritta l'11 dicembre 2025;

LE PARTI CONCORDANO CHE

Art. 1 - Finalità

L'Ateneo, in funzione delle proprie esigenze organizzative e funzionali e nel pieno rispetto dello Statuto dei Lavoratori, adotta Strumenti e Servizi ICT che, seppur indirettamente, potrebbero consentire forme di controllo a distanza (cosiddetto controllo preterintenzionale) e il trattamento di dati personali relativi ai/alle lavoratori/trici attraverso sistemi che generano, raccolgono e conservano log e metadati.

L'Ateneo garantisce che l'utilizzo di tali strumenti e servizi informatici non sia finalizzato a controlli sistematici o preordinati sulla diligenza del personale in relazione al rispetto dell'orario di lavoro (ad eccezione dei sistemi specifici per la rilevazione delle presenze) o sulla correttezza nello svolgimento della prestazione lavorativa. Nella gestione dei controlli su Strumenti e Servizi ICT viene posta particolare attenzione ad evitare qualsiasi limitazione ingiustificata dei diritti e delle libertà fondamentali dei/delle lavoratori/trici.

Le analisi preventive saranno svolte in maniera prevalentemente automatizzata, al fine di segnalare eventuali anomalie. A titolo esemplificativo, tali analisi possono includere:

1) raccolta dei log di accesso ai sistemi per rilevare accessi non autorizzati;
2) analisi automatica del traffico di rete per identificare malware o attività sospette;
3) verifica dello stato di aggiornamento dei software e dei dispositivi;
4) analisi di integrità dei dati e backup.

Ogni eventuale analisi successiva sarà effettuata esclusivamente lato tecnico e da personale autorizzato, con finalità di sicurezza informatica, manutenzione dei sistemi, risoluzione di anomalie, ricostruzione di incidenti di sicurezza o gestione delle risorse digitali.

Tali attività non sono in alcun modo finalizzate alla valutazione della prestazione lavorativa individuale, né al controllo dell'orario o della produttività, e sono condotte nel rispetto dei principi di pertinenza, non eccedenza e tutela dei diritti fondamentali dei/delle lavoratori/trici.

L'uso degli strumenti e delle credenziali ICT forniti è sotto la responsabilità diretta dell'assegnatario. La raccolta automatica di metadati e log ha come finalità esclusiva quella di garantire il regolare funzionamento e la continuità operativa dei sistemi e dei servizi informatici e di telecomunicazione, verificarne la funzionalità, tutelarne la sicurezza e preservare l'integrità degli strumenti e dei dati. Inoltre, tali attività consentono di prevenire la messa in atto e la reiterazione di illeciti, soddisfare esigenze difensive, assicurare la tempestiva gestione di incidenti di sicurezza o violazioni dei dati personali, nonché analizzare eventi dannosi e le relative cause al fine di migliorare le procedure di verifica e tutela del sistema e degli strumenti, a salvaguardia anche dell'utente stesso.

Il trattamento dei dati è riservato esclusivamente a soggetti appositamente incaricati (Amministratori di Sistema, soggetti autorizzati al trattamento e personale del Fornitore dei servizi formalmente designato come Responsabile del trattamento), nel rispetto della normativa vigente in materia di protezione dei dati personali e, ove opportuno, del principio di segretezza della corrispondenza. È quindi espressamente escluso ogni controllo diretto sul contenuto della

posta elettronica o di altre forme di corrispondenza telematica da parte degli Amministratori di sistema o di altri incaricati del trattamento.

Art. 2 Principi

Le parti convengono che l'utilizzo degli strumenti e servizi infotelematici di seguito elencati all'art. 3, avverrà in conformità a quanto stabilito dall'art. 4 dello Statuto dei Lavoratori e della normativa in materia di protezione dei dati personali, precisando, in particolare, che le apparecchiature non saranno in alcun modo utilizzate quale strumento di controllo a distanza della prestazione del personale.

È fatta salva, in ogni caso, l'applicazione delle norme che impongono obblighi di segnalazione alle competenti Autorità o di attivazione di procedure di competenza del datore di lavoro nel caso di accertata responsabilità del/della lavoratore/trice per le condotte che hanno determinato danni o pericoli per il patrimonio dell'Amministrazione dovute all'inosservanza o violazione delle norme vigenti e delle prescrizioni impartite.

Art. 3 Tipologie di metadati/log e tempi di conservazione

In conformità alle finalità sopra menzionate, di seguito vengono riportate le tipologie di metadati e log, suddivise per macrocategorie, i relativi tempi massimi di conservazione e le modalità di raccolta attraverso la registrazione degli eventi sui sistemi informatici gestiti direttamente dalla Direzione ICT (l*ogging*), nonché l'eventuale controllo in presenza di anomalie.

Trascorsi i termini indicati, la conservazione e l'utilizzo dei metadati e dei log non sono consentiti, fatta eccezione per ordini provenienti dall'Autorità competente, controversie legali in corso o attivazione di procedure di pertinenza del datore di lavoro nei casi di responsabilità accertata del lavoratore, o periodi di conservazione previsti da disposizioni normative.

Tipi di metadati/log e relativi tempi di conservazione:

1. il servizio di posta elettronica genera log tecnici relativi alle operazioni effettuate sui messaggi, tra cui: creazione, modifica, invio, ricezione, lettura, risposta, inoltro, cancellazione, spostamento tra cartelle, accesso da dispositivi o client diversi, e altre operazioni equivalenti. I log includono: indirizzi e-mail del mittente e del destinatario, indirizzi IP dei client e dei server coinvolti, data e ora dell'operazione, tipo di operazione, oggetto del messaggio, dimensione del messaggio, presenza e dimensione degli eventuali allegati, identificativo del messaggio, protocollo utilizzato e client/dispositivo di accesso. La conservazione dei suddetti log è prevista per un periodo di **90 giorni;**
2. l'utilizzo degli strumenti per la produttività individuale (es. Microsoft Word, Excel, Teams, Outlook, OneDrive, SharePoint) genera log tecnici relativi alle operazioni effettuate dagli utenti, tra cui: apertura e modifica di documenti, invio e ricezione di messaggi, condivisione di file, accesso a contenuti, sincronizzazione tra dispositivi, e altre attività equivalenti. I log includono: lo strumento utilizzato, il tipo di operazione svolta, la data e l'orario dell'azione, l'indirizzo IP del dispositivo e l'area geografica associata, le informazioni sul dispositivo (marca, modello, sistema operativo, nome del device), il tipo di autenticazione eseguita, l'identità dell'utente, il client o protocollo utilizzato, lo stato dell'operazione, eventuali modifiche ai permessi o condivisioni, e le azioni amministrative eventualmente eseguite. Questi log sono conservati per un periodo di **90 giorni;**

3. i sistemi anti-malware generano: ID di origine del log (nome utente o dispositivo), ID destinazione pertinente e appropriato per il tipo di evento, data e ora dell'evento, dettagli (tipo di evento, risultato delle analisi o delle automazioni, informazioni dettagliate definite in base all'evento), protocolli e indirizzi di rete di origine e di destinazione pertinenti e appropriati per il tipo di evento e se previsti. I tempi di conservazione di tali log è pari a **180 giorni;**
4. l'utilizzo della soluzione per la gestione degli endpoint genera log tecnici relativi alle attività di configurazione, registrazione, monitoraggio, protezione e conformità dei dispositivi aziendali. Tali log includono: l'identificativo del dispositivo, il sistema operativo, la versione del software, il tipo di connessione, l'indirizzo IP, l'area geografica associata, l'identità dell'utente associato al dispositivo, le operazioni effettuate (es. registrazione, aggiornamento, installazione o rimozione di applicazioni, applicazione di criteri di sicurezza, modifica delle configurazioni), il tipo di autenticazione eseguita, lo stato delle operazioni e le eventuali azioni correttive o di conformità. I log delle operazioni utente sono conservati per un periodo di **90 giorni**, mentre i log dei dispositivi (es. nome dispositivo, utente primario, data di ultimo contatto) sono conservati **fino a 24 mesi**. Questo periodo di conservazione è necessario per garantire la gestione del ciclo di vita del dispositivo e il relativo inventario;
5. I sistemi di gestione delle identità digitali che, l'Ateneo utilizza, prevedono la sincronizzazione tra il dominio locale (on-premises) e la piattaforma cloud. L'autenticazione degli utenti avviene tramite modalità pass-through, con validazione delle credenziali direttamente sul Domain Controller locale. I log tecnici generati da questi sistemi includono: l'identità dell'utente, il tipo di operazione effettuata (es. autenticazione, sincronizzazione, modifica di attributi, creazione o disabilitazione di account), la data e l'orario dell'operazione, l'indirizzo IP del dispositivo, l'area geografica associata, il tipo di autenticazione eseguita, il dispositivo e il client utilizzato, lo stato dell'operazione e le eventuali azioni amministrative. Tali log sono conservati per un periodo di **90 giorni**;
6. i sistemi di monitoraggio delle reti e gestione del servizio VPN (firewall) generano:
    a. log e metadati relativi al traffico: data e ora dell'evento, IP sorgente, IP destinazione, eventuale nome utente (previsto solo nelle casistiche di navigazione in VPN, WiFi o tramite l'uso di account sulle postazioni UniCloud), porte e protocolli utilizzati, URL visitata e file oggetto del traffico se pertinenti al tipo di evento;
    b. log e metadati relativi al servizio VPN: data e ora dell'evento, tipo di evento (e.g. login e logout), IP da cui viene instaurato il tunnel e IP assegnato dal servizio, paese da cui viene instaurato il tunnel, nome utente associato all'evento, informazioni sul dispositivo (client utilizzato e sua versione, sistema operativo, nome del dispositivo). Il periodo di conservazione per i suddetti log e metadati è pari a **180 giorni**;
7. i sistemi di Data Loss Prevention (DLP) utilizzati sono finalizzati alla protezione dei dati sensibili e alla prevenzione di condivisioni non autorizzate. I log tecnici generati da tali sistemi riguardano le attività di accesso e autenticazione, le modifiche ai permessi e alle configurazioni, le operazioni su file e documenti (creazione, modifica, eliminazione), le attività svolte su e-mail e calendari, le azioni effettuate sulle applicazioni registrate e sui

servizi cloud, nonché il nome utente associato a ciascuna operazione. I log sono conservati per un periodo di **180 giorni;**

8. Il sistema SIEM (*Security Information and Event Management*) raccoglie log e metadati da vari strumenti e servizi ICT critici, come quelli oggetto di questo accordo, per rilevare e gestire rapidamente gli incidenti informatici, generando solo i log infrastrutturali necessari senza produrre ulteriori registrazioni sugli utenti. Tutti i log e metadati citati nei punti precedenti possono essere ingeriti dal servizio e quindi fanno parte del suo ecosistema. Il tempo di conservazione massima di tali log e metadati è di **180 giorni**;
9. il sistema di stampa centralizzata genera i seguenti log: nome macchina, nome utente, data/ora dell'operazione, riferimento del documento stampato. Al momento, questo tipo di dato viene conservato in modalità circolare e quindi i nuovi log vanno a sovrascrivere i più vecchi quando lo spazio non è sufficiente. La Direzione ICT si impegna a definire una procedura per cancellare i log entro un tempo stabilito e inferiore a **180 giorni**.

Per quanto riguarda i metadati che vengono incorporati nei documenti, si applicano le disposizioni normative vigenti e i tempi previsti per la conservazione dei documenti dalla pubblica amministrazione.

Art. 4 Raccolta e monitoraggio ed eventuali controlli

Gli strumenti e i servizi ICT sono provvisti di sistemi automatizzati di analisi, finalizzati a garantire gli obiettivi indicati in premessa. Tali sistemi bloccano operazioni potenzialmente rischiose, incluse quelle effettuate dagli utenti, e raccolgono automaticamente log tecnici e metadati. La gestione dei log è strutturata in modo da assicurare il rispetto delle vigenti normative sulla protezione dei dati personali, come illustrato nel paragrafo precedente. Il primo livello di controllo ordinario si fonda, talvolta, sull'utilizzo di filtri preventivi preconfigurati che riducono la probabilità di incidenti di sicurezza. Ad esempio, i firewall impediscono l'accesso a siti web con contenuti illeciti; il sistema automatico di filtraggio delle e-mail (antispam, quarantena di file identificati come pericolosi, ecc.) previene la consegna agli utenti di messaggi potenzialmente dannosi. Entrambi i sistemi generano notifiche automatiche di anomalia (come alert relativi al download di file o navigazione verso domini associati ad attività malevole quali phishing), le quali possono essere analizzate successivamente dal personale autorizzato. I sistemi di filtraggio, per classificare e prevenire incidenti – come quelli relativi a e-mail di phishing – devono essere in grado di analizzare in modo automatico il contenuto dei messaggi, senza ricorrere al diretto intervento degli Amministratori di Sistema o di altre figure incaricate del trattamento dei dati.

Analisi tecnico-funzionali più approfondite vengono avviate qualora dal controllo ordinario emergano ripetute anomalie – inclusi indicatori di malfunzionamento dei sistemi informativi e delle reti dell'Ateneo – tali da mettere a rischio o violare i principi di integrità, riservatezza e disponibilità dei dati, dei servizi informativi e delle reti stesse, con possibile compromissione della corretta funzionalità e integrità degli strumenti e servizi. In presenza di un'anomalia rilevata, come la presenza di malware su un dispositivo, la violazione di regolamenti e politiche d'uso degli strumenti e servizi, o una segnalazione dell'utente stesso (es. furto o smarrimento degli strumenti aziendali), il personale tecnico incaricato può:

- bloccare l'accesso alla rete o a specifici servizi interni/esterni per limitare le conseguenze dell'incidente;

- svolgere analisi sui log di accesso, sulle postazioni di lavoro o sugli asset assegnati dall'Ateneo per individuare eventuali accessi non autorizzati, compromissioni dei sistemi, identificare la natura del problema e pianificare adeguate contromisure;
- impostare l'obbligo di cambio password per l'account dell'utente.

Nel caso il personale autorizzato rilevi anomalie o incidenti, potrà essere avviato un controllo generale o specifico su alcune aree dell'infrastruttura digitale dell'Ateneo. Se necessario, questa attività può concludersi con la diffusione di un avviso generale riguardante l'utilizzo anomalo degli strumenti e servizi ICT, invitando gli utenti a seguire scrupolosamente le indicazioni del personale autorizzato. L'avviso può essere destinato solo a un gruppo più ristretto di utenti, ma senza identificazione puntuale dell'utente che ha generato l'anomalia. In assenza di ulteriori anomalie, salvo eccezioni debitamente motivate, non si giustifica lo svolgimento di controlli individuali.

Nel caso in cui sia necessario effettuare analisi individuali a seguito di incidenti informatici, tali attività vengono condotte esclusivamente per le finalità correlate alla risoluzione dell'incidente e, se possibile, con il coinvolgimento diretto degli utenti interessati, al fine di garantire trasparenza, informazione e contraddittorio. Gli utenti e le relative strutture di appartenenza sono tenuti a collaborare affinché il personale tecnico possa intervenire rapidamente ed efficacemente sul contenimento e sulla risoluzione dell'impatto, facilitando il tempestivo ripristino delle condizioni di normalità. Accertamenti possono altresì essere richiesti dall'interessato o dall'Autorità giudiziaria competente. È esclusa qualsiasi altra finalità, diretta o indiretta, di controllo a distanza dell'attività lavorativa del personale o l'impiego dei log per scopi diversi da quelli previsti dal presente Accordo, salvo quanto disposto da norme di legge specifiche o da provvedimenti delle Autorità competenti.

Qualora vengano riscontrate violazioni delle normative nazionali o degli atti adottati dall'Ateneo nel rapporto di lavoro con le amministrazioni pubbliche, gli uffici competenti daranno corso agli adempimenti necessari. In ogni circostanza, l'Ateneo si riserva la facoltà di intraprendere azioni immediate in situazioni di emergenza che comportino rischi concreti e attuali di violazione dei principi di integrità, riservatezza e disponibilità dei dati e dei servizi ICT.

Art. 5 Formazione e comunicazione

Le Parti convengono sulla necessità di una significativa campagna di formazione a tutto il personale con l'obiettivo di illustrare le regole e i comportamenti da tenere al fine di garantire la sicurezza dei sistemi informativi e di prevenire comportamenti contestabili.

Le parti convengono, infine, sull'indispensabilità di una capillare informazione e comunicazione sulle finalità dei controlli e sulle modalità con cui gli stessi sono esercitati, al fine di ottemperare al principio di massima trasparenza.

Art. 6 Norme finali

Il presente Accordo è oggetto di revisione annuale, anche al fine di valutare la progressiva riduzione dei tempi di conservazione dei metadati ivi previsti.

Fermo restando quanto previsto ai punti precedenti, qualora intervengano modifiche di natura normativa, contrattuale o tecnica, in particolare sulla riduzione dei tempi di conservazione dei

metadati, l'Amministrazione si impegna a informare la Parte Sindacale e provvede a riconvocare tempestivamente il tavolo sindacale per valutare eventuali modifiche all'Accordo.

Infine, in caso di successive modifiche o implementazioni sui sistemi di sicurezza o di revisioni alle Disposizioni sull'utilizzo degli strumenti e dei servizi infotelematici, la Parte Sindacale sarà preventivamente informate.

PER LA PARTE PUBBLICA

Prof.ssa Marina Brambilla

La Rettrice dell'Università degli Studi di Milano

MARINA MARZIA BRAMBILLA
Universita' degli Studi di Milano
22.12.2025 09:55:43
GMT+01:00

Dott. Angelo Casertano

Il Direttore Generale

ANGELO PASQUALE CASERTANO
UNIVERSITÀ DEGLI STUDI DI MILANO
19.12.2025 14:22:58
GMT+01:00

PER LE ORGANIZZAZIONI SINDACALI

FLC CGIL

Sara Carrapa

Sara Carrapa
Universita' degli Studi di Milano
23.12.2025 12:45:40
GMT+02:00

CISL FSUR

Angela Gambirasio

Angela Gambirasio
Universita' degli Studi di Milano
23.12.2025 17:04:16
GMT+00:00

SNALS-CONFSAL

Ernesto Gandini

Ernesto Gandini
Università degli Studi di Milano
23.12.2025 14:47:31
GMT+02:00

ANIEF

Daniela Diana

Daniela Diana
Universita' degli Studi di Milano
23.12.2025 12:23:10
GMT+01:00

PER LA R.S.U.

Alberto Airoldi
Universita' degli Studi di Milano
22.12.2025 11:34:33
GMT+00:00

PAOLA LANGUZZI
UNIVERSITÀ DEGLI STUDI DI MILANO
23.12.2025 15:07:23
GMT+01:00

Rocco Maria Marzulli
Universita' degli Studi di Milano
23.12.2025 16:39:02
GMT+02:00