DELIBERA DEL CONSIGLIO DI AMMINISTRAZIONE

N. 22 DEL 07.07.2026

L'anno 2026 il giorno 7 luglio alle ore 14.00 presso la sede di Via dell'Artigliere n. 9 a seguito di regolare convocazione si è riunito il Consiglio di Amministrazione dell'ESU di Verona

OGGETTO: **Aggiornamento del "Regolamento per l'utilizzo degli strumenti aziendali" dell'ESU di Verona**

CONSIGLIERI

		P	A
1	Cau Sergio		X
2	Gottin Leonardo	X	
3	Miceli Sopo Francesco	X	
4	Valente Claudio	X	
5	----------*		

***** il consigliere Facci Daniele in data 07.01.2025 ha rassegnato le dimissioni ed è in corso la procedura di nomina del nuovo rappresentante del Consiglio Regionale.

PRESIDENTE Valente Claudio

SEGRETARIO Gugole Giorgio

COLLEGIO DEI REVISORI CONTI

Dal Dosso Davide Tommaso
Gambaretto Nicola
Simonato Flavio

IL CONSIGLIO DI AMMINISTRAZIONE

Sentita la relazione del Presidente che illustra l'argomento posto all'ordine del giorno:

PREMESSO che il presente regolamento disciplina le modalità di utilizzo degli strumenti informatici, telematici e digitali messi a disposizione dall'ESU di Verona, nonché le connesse misure organizzative, tecniche e di sicurezza, al fine di assicurarne il corretto impiego per finalità istituzionali, la tutela del patrimonio informativo dell'Ente, la continuità operativa, nonché la protezione dei dati personali trattati nell'ambito delle attività istituzionali;

CONSIDERATO che le disposizioni del presente regolamento si applicano al personale dipendente, ai dirigenti, ai collaboratori, ai lavoratori somministrati, ai tirocinanti, ai soggetti in distacco, ai consulenti, nonché a ogni altro soggetto autorizzato, anche temporaneamente, all'uso degli strumenti e servizi informatici dell'Ente;

CONSIDERATO che le medesime disposizioni si applicano, in quanto compatibili, anche ai soggetti esterni che accedano ai sistemi, alle reti o alle dotazioni dell'ESU di Verona per esigenze connesse allo svolgimento di attività istituzionali, contrattuali o di supporto;

CONSIDERATO che il presente regolamento si adotta nel quadro della normativa europea e nazionale vigente e, in particolare, tiene conto delle seguenti fonti:

- Statuto dei Lavoratori (Legge 300/1970) - Articolo 4
- Codice di Comportamento dei Dipendenti Pubblici (DPR 62/2013 e successive modifiche)
- Testo Unico sul Pubblico Impiego (D.Lgs. 165/2001) e CCNL Funzioni Locali
- GDPR (Regolamento UE 2016/679)
- Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 aggiornato dal D.Lgs. 101/2018)
- Codice dell'Amministrazione Digitale (CAD - D.Lgs. 82/2005)
- Piano Triennale per l'Informatica nella PA (AgID)
- Direttive dell'Agenzia per la Cybersicurezza Nazionale (ACN) e Direttiva NIS2
- Legge 81/2017 sul Lavoro Agile

Tutto ciò premesso e considerato.

VISTO decreto legislativo 29 marzo 2012, n. 68;

VISTO il DPCM 9 aprile 2001;

VISTO la legge regionale 7 aprile 1998, n. 8;

Sottoposta a votazione la presente deliberazione risulta così approvata:

- Consiglieri presenti N. 3
- Consiglieri votanti N. 3
- Voti favorevoli N. 3
- Voti contrari N. =
- Astenuti N. =

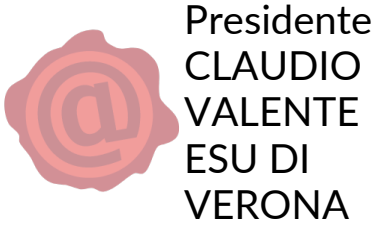
D E L I B E R A

1. di considerare le premesse parte integrante del presente provvedimento;
2. di approvare il " Regolamento per l'utilizzo degli strumenti aziendali " dell'ESU di Verona;
3. di demandare al Direttore dell'ESU ogni provvedimento conseguente all'approvazione e all'attuazione della presente deliberazione;
4. di individuare quale responsabile del procedimento il Dirigente dott. Luca Bertaiola – Direzione Benefici e Servizi agli Studenti dell'ESU di Verona;
5. di trasmettere il presente provvedimento al responsabile del servizio "Albo on line" per i provvedimenti di competenza;

Atto non soggetto a controllo ai sensi della Legge Regionale 7 aprile 1998, n.8.

IL SEGRETARIO
(dott. Giorgio Gugole)

IL PRESIDENTE
(dott. Claudio Valente)



UFFICIO RAGIONERIA

Visto ed assunto l'impegno di €. _____ sul cap. _____

del Conto [R] / [C] del Bilancio _____

al n. _____ ai sensi dell'art. 43 L.R. 29.11.2001 n.39

Verona, _____

IL RAGIONIERE

_____

SEGRETERIA

Si attesta che la presente delibera, di cui questa è copia conforme all'originale per uso amministrativo, è stata trasmessa in data odierna all'Amministrazione Regionale.

Verona, _____ IL DIRETTORE

_____

La presente delibera è divenuta esecutiva a seguito di controllo da parte della Giunta Regionale in data _____.

Verona, _____ IL DIRETTORE

_____

La presente delibera è pubblicata all'albo ufficiale dell'Ente dal giorno _____.

IL DIRETTORE

_____

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI AZIENDALI

INDICE

Art. 1 – Oggetto

1. Il presente regolamento disciplina le modalità di utilizzo degli strumenti informatici, telematici e digitali messi a disposizione dall'ESU di Verona, nonché le connesse misure organizzative, tecniche e di sicurezza, al fine di assicurarne il corretto impiego per finalità istituzionali, la tutela del patrimonio informativo dell'Ente, la continuità operativa, nonché la protezione dei dati personali trattati nell'ambito delle attività istituzionali.
2. Il regolamento costituisce parte integrante del sistema di regole interne dell'Ente e si applica ai soggetti che, a qualunque titolo, utilizzino le risorse informatiche e telematiche dell'ESU di Verona.

Art. 2 – Ambito di applicazione

1. Le disposizioni del presente regolamento si applicano al personale dipendente, ai dirigenti, ai collaboratori, ai lavoratori somministrati, ai tirocinanti, ai soggetti in distacco, ai consulenti, nonché a ogni altro soggetto autorizzato, anche temporaneamente, all'uso degli strumenti e servizi informatici dell'Ente.
2. Le medesime disposizioni si applicano, in quanto compatibili, anche ai soggetti esterni che accedano ai sistemi, alle reti o alle dotazioni dell'ESU di Verona per esigenze connesse allo svolgimento di attività istituzionali, contrattuali o di supporto.

Art. 3 – Principi generali

1. L'utilizzo degli strumenti aziendali deve avvenire nel rispetto dei principi di diligenza, correttezza, lealtà, proporzionalità e riservatezza.
2. Gli strumenti messi a disposizione dall'Ente devono essere utilizzati, di norma, esclusivamente per finalità connesse all'esecuzione della prestazione lavorativa o allo svolgimento dell'attività istituzionale.
3. È consentito un uso personale meramente occasionale e contenuto, purché non arrechi pregiudizio all'organizzazione del servizio, alla sicurezza dei sistemi, alla funzionalità delle risorse, alla reputazione dell'Ente o al corretto adempimento degli obblighi di servizio.
4. È fatto divieto di utilizzare le dotazioni e i servizi dell'Ente per attività illecite, offensive, discriminatorie, diffamatorie, fraudolente o comunque contrarie alla legge, ai contratti collettivi, alle disposizioni interne e alle finalità istituzionali.

Art. 4 – Dotazioni e responsabilità

1. Le dotazioni hardware e software concesse in uso restano nella disponibilità dell'Ente, salvo diversa previsione contrattuale o regolamentare.
2. Ciascun assegnatario è tenuto a custodire con diligenza i beni ricevuti e a farne uso secondo le istruzioni impartite dall'Ente e le regole tecniche di sicurezza vigenti.

3. È vietata la manomissione, modifica, alterazione o integrazione non autorizzata delle configurazioni hardware e software, nonché l'installazione di applicativi, componenti, periferiche, servizi o dispositivi non preventivamente autorizzati.
4. Ogni anomalia, guasto, sottrazione, smarrimento, deterioramento, sospetta compromissione o evento potenzialmente pregiudizievole deve essere immediatamente segnalato ai soggetti competenti secondo le procedure interne.

Art. 5 – Sicurezza dei sistemi

1. I sistemi, gli apparati e le applicazioni informatiche devono essere protetti mediante adeguate misure di sicurezza, tra le quali, ove previste, autenticazione personale, autenticazione multifattore, cifratura dei dispositivi, blocco automatico della sessione, aggiornamenti periodici e strumenti di protezione perimetrale.
2. È fatto divieto di disattivare, eludere, modificare o ridurre l'efficacia dei sistemi di protezione, controllo e sicurezza predisposti dall'Ente.
3. I dispositivi mobili e i sistemi portatili devono essere utilizzati nel rispetto delle misure minime di sicurezza e delle eventuali ulteriori misure stabilite dall'Ente, anche mediante sistemi di gestione centralizzata.

Art. 6 – Credenziali di autenticazione

1. Le credenziali di accesso sono personali, riservate e strettamente individuali; esse non possono essere cedute, comunicate o rese accessibili a terzi.
2. L'utente è responsabile della custodia e dell'utilizzo delle proprie credenziali, nonché di ogni attività compiuta mediante le medesime, salvo i casi di uso indebito imputabili a terzi e tempestivamente segnalati secondo le procedure interne.
3. Le password devono rispondere ai requisiti di robustezza previsti dalle procedure dell'Ente e devono essere sostituite nei casi previsti o quando vi sia ragione di ritenere che la loro riservatezza sia venuta meno. Le password per l'accesso al computer sono cambiate con cadenza trimestrale.
4. È fatto divieto di annotare le credenziali in forma non sicura, di trasmetterle mediante canali non autorizzati o di conservarle in documenti o supporti non protetti.

Art. 7 – Postazioni di lavoro e dispositivi mobili

1. Le postazioni di lavoro devono essere utilizzate in modo tale da prevenire accessi non autorizzati, consultazioni indebite, alterazioni, cancellazioni o diffusioni non consentite di dati e documenti.
2. In caso di allontanamento temporaneo dalla postazione, il dipendente o l'utilizzatore è tenuto a inserire manualmente l'impostazione di sicurezza per bloccare la sessione di lavoro e ad adottare ogni misura idonea a impedire la visione o l'utilizzo della postazione da parte di terzi.
3. I dispositivi portatili e mobili eventualmente assegnati devono essere custoditi con la massima attenzione, specialmente al di fuori delle sedi dell'Ente. I dispositivi devono essere

protetti con sistemi di blocco quali password, pin, impronta digitale che impediscano l'accesso ad altre persone.
4. È vietato il collegamento alla rete o ai sistemi dell'Ente di dispositivi personali non autorizzati, salvo espressa previsione organizzativa o tecnica.

Art. 8 – Utilizzo della rete internet

1. L'accesso alla rete internet è consentito per finalità istituzionali, lavorative e di servizio, in coerenza con le mansioni svolte e con le esigenze organizzative dell'Ente.
2. È vietata la navigazione verso siti o servizi che possano compromettere la sicurezza dei sistemi, determinare la violazione di obblighi di legge o esporre l'Ente a rischi di natura tecnica, patrimoniale o reputazionale.
3. L'Ente può adottare misure di filtraggio, limitazione, registrazione o monitoraggio tecnico della navigazione, nei limiti consentiti dalla normativa vigente e per le sole finalità di sicurezza, manutenzione, continuità operativa e tutela del patrimonio informativo.

Art. 9 – Posta elettronica e strumenti di collaborazione

1. La posta elettronica istituzionale deve essere utilizzata esclusivamente per finalità connesse all'attività di servizio.
2. È vietato l'utilizzo della casella di posta elettronica istituzionale per finalità private, salvo eventuale diversa regolamentazione espressamente autorizzata dall'Ente nei limiti di legge.
3. È fatto obbligo di prestare particolare attenzione all'apertura di allegati, link, messaggi o contenuti provenienti da mittenti non conosciuti o sospetti, nonché a richieste anomale di dati, credenziali, codici o informazioni riservate.
4. L'utilizzo di strumenti di videoconferenza, messaggistica istantanea, collaborazione online, archiviazione cloud o altri servizi digitali di terzi è consentito esclusivamente se previamente autorizzato e configurato secondo le misure di sicurezza definite dall'Ente.

Art. 10 – Trattamento dei dati personali e riservatezza

1. I soggetti destinatari del presente regolamento sono tenuti a trattare i dati personali e le informazioni di cui vengano a conoscenza in ragione del servizio o dell'attività svolta esclusivamente nei limiti delle autorizzazioni ricevute e secondo il principio di necessità.
2. È vietata ogni diffusione, comunicazione o utilizzazione non autorizzata di dati, documenti, immagini, schermate, archivi o informazioni appartenenti all'Ente o riferibili a terzi.
3. Qualora un soggetto riceva per errore dati o documenti non destinati alla propria conoscenza, deve cessarne immediatamente la consultazione e darne tempestiva comunicazione ai soggetti competenti.

Art. 11 – Lavoro agile e accesso remoto

1. L'accesso da remoto ai sistemi dell'Ente è consentito esclusivamente attraverso strumenti, canali e procedure autorizzati.

2. Nell'ambito delle attività svolte in modalità agile o da remoto, l'utilizzatore è tenuto ad adottare ogni cautela idonea a garantire la riservatezza delle informazioni trattate, la protezione dei dispositivi e la sicurezza delle connessioni.
3. È vietato l'utilizzo di reti, applicazioni, servizi o dispositivi non autorizzati quando ciò possa compromettere la sicurezza delle informazioni o dei sistemi dell'Ente.

Art. 12 – Controlli tecnici e garanzie

1. L'Ente può effettuare controlli tecnici, diagnostici e di sicurezza sugli strumenti assegnati, nei limiti e per le finalità consentite dalla normativa vigente, in particolare per esigenze di sicurezza, manutenzione, continuità operativa, tutela del patrimonio informativo e verifica del corretto funzionamento dei sistemi.
2. I controlli devono essere effettuati nel rispetto dei principi di necessità, proporzionalità, minimizzazione e trasparenza, evitando forme di sorveglianza occulta o generalizzata non consentite.
3. I log tecnici, i registri di accesso e gli ulteriori dati di funzionamento dei sistemi sono conservati per il tempo strettamente necessario alle finalità per le quali sono raccolti, secondo la disciplina interna e nel rispetto della normativa in materia di protezione dei dati personali.

Art. 13 – Incidenti di sicurezza e data breach

1. Ogni evento anomalo, accesso abusivo, sospetta compromissione, perdita, sottrazione, distruzione, alterazione, divulgazione non autorizzata o altro incidente di sicurezza deve essere immediatamente segnalato secondo le procedure interne.
2. I destinatari del presente regolamento sono tenuti a collaborare con le strutture competenti per la gestione dell'incidente, la mitigazione degli effetti, il ripristino delle funzionalità e la conservazione degli elementi utili alle verifiche tecniche e organizzative.

Art. 14 – Cessazione del rapporto, restituzione e conservazione

1. Alla cessazione del rapporto di servizio, ovvero al venir meno, per qualsiasi causa, dell'abilitazione all'uso, l'interessato è tenuto a restituire senza indugio i beni, le credenziali, i supporti, i dispositivi e ogni altro elemento affidato dall'Ente.
2. L'Ente provvede, secondo le procedure interne e nel rispetto della normativa applicabile, alla messa in sicurezza, al recupero, alla cancellazione o al trasferimento dei dati contenuti nei dispositivi e negli archivi assegnati.
3. Eventuali ulteriori esigenze di conservazione sono ammesse nei soli casi previsti dalla legge o per la tutela di un diritto in sede giudiziaria, fermo restando il rispetto dei principi di limitazione della conservazione e minimizzazione.

Art. 15 – Violazioni e sanzioni

1. La violazione delle disposizioni del presente regolamento comporta l'applicazione delle misure e delle conseguenze previste dalla normativa vigente, dai contratti collettivi applicabili e dagli atti interni dell'Ente.
2. Restano fermi gli eventuali profili di responsabilità disciplinare, amministrativa, civile e penale derivanti da condotte illecite o da utilizzi impropri degli strumenti informatici e telematici.

Art. 16 – Aggiornamento e pubblicità

1. Il presente regolamento è oggetto di revisione periodica in relazione all'evoluzione tecnologica, organizzativa e normativa.
2. Esso è reso conoscibile a tutto il personale e agli altri soggetti interessati mediante i canali istituzionali dell'Ente ed è efficace dalla data stabilita nell'atto di approvazione.

ALLEGATO TECNICO-OPERATIVO

Finalità e ambito

Il presente allegato tecnico-operativo definisce le misure minime organizzative e tecniche, le istruzioni operative e i criteri di gestione applicabili all'utilizzo delle dotazioni informatiche, telematiche e digitali dell'Ente. Esso integra il regolamento principale e ne costituisce parte sostanziale, con funzione di supporto applicativo e di aggiornamento operativo coerente con l'evoluzione tecnologica e normativa.

Le disposizioni del presente allegato si applicano a tutto il personale dipendente, ai dirigenti, ai collaboratori, ai consulenti e a ogni altro soggetto autorizzato all'uso delle risorse digitali dell'Ente, nei limiti di compatibilità con il relativo rapporto giuridico e con le funzioni concretamente esercitate.

Classificazione delle risorse

Ai fini del presente allegato, le risorse dell'Ente si distinguono in: dispositivi fissi e mobili, reti e connettività, sistemi applicativi, account e credenziali, servizi cloud e piattaforme collaborative, archivi documentali, sistemi di posta elettronica, strumenti di videoconferenza, log di sicurezza e supporti di memorizzazione.

Le informazioni trattate mediante tali risorse devono essere classificate almeno nelle seguenti categorie: pubbliche, ad uso interno, riservate, contenenti dati personali particolari o comunque richiedenti misure rafforzate di protezione. Le modalità di accesso, condivisione, trasmissione e conservazione devono essere commisurate alla classificazione attribuita.

Misure minime di sicurezza

Devono essere adottate, mantenute e periodicamente verificate almeno le seguenti misure minime:

- autenticazione individuale per tutti gli utenti;
- autenticazione multifattore per accessi remoti, utenze privilegiate e applicazioni critiche;
- blocco automatico della sessione dopo un periodo di inattività definito dall'Ente;
- aggiornamento periodico di sistemi operativi, applicativi e componenti di sicurezza;
- protezione antimalware, antispam, antiphishing e firewall secondo gli standard adottati dall'Ente;
- sistemi di backup periodico, del server e di tutti gli applicativi (no pc, portatili e cellulari) dell'Ente con verifica dell'integrità delle copie e test di ripristino;
- profilazione degli accessi secondo i principi di necessità, minimizzazione e segregazione dei compiti;
- tracciamento tecnico degli eventi rilevanti di sicurezza nei limiti consentiti dalla normativa;
- inventario aggiornato delle dotazioni hardware, software e dei servizi digitali autorizzati.

Le misure sopra indicate devono essere attuate in modo proporzionato ai rischi, alla tipologia dei dati trattati, al ruolo dell'utente e alla criticità dei servizi interessati.

Gestione delle credenziali

Le credenziali di autenticazione sono strettamente personali e non possono essere cedute, condivise o custodite in forma non sicura. Le password devono rispettare i requisiti di complessità previsti dalle procedure interne e devono essere modificate in caso di sospetta compromissione, uso indebito o a seguito di specifica richiesta dell'Ente.

Per le utenze amministrative, tecniche o ad alto privilegio devono essere previste misure rafforzate, con eventuale autenticazione multifattore, separazione degli account ordinari dagli account privilegiati, tracciamento degli accessi e limitazione dell'uso ai soli casi necessari.

Postazioni di lavoro

Le postazioni di lavoro devono essere configurate secondo standard approvati dall'Ente e non possono essere alterate dall'utente senza preventiva autorizzazione. In caso di assenza, anche temporanea, l'utente è tenuto a bloccare la sessione e a sottrarre alla vista documenti o informazioni riservate.

Documenti cartacei, stampe e supporti rimovibili contenenti dati o informazioni di servizio non devono essere lasciati incustoditi presso la postazione. Al termine dell'orario di lavoro, gli utenti devono adottare misure coerenti con il principio di clean desk e con le disposizioni interne in materia di sicurezza fisica.

Dispositivi mobili e portatili

Notebook, smartphone e tablet assegnati dall'Ente devono essere protetti mediante PIN o password robusta, cifratura, blocco automatico e, ove previsto, sistemi di gestione centralizzata. È vietata la rimozione dei profili di sicurezza installati dall'Ente.

In caso di utilizzo fuori sede, l'utente deve evitare l'esposizione del dispositivo a furto, smarrimento, manomissione o accesso da parte di terzi. In caso di furto, perdita o sospetta compromissione, è obbligatoria l'immediata segnalazione ai referenti competenti, al fine di consentire l'adozione delle misure di contenimento, inclusa, se disponibile, la cancellazione remota.

Accesso remoto e lavoro agile

L'accesso remoto ai sistemi dell'Ente è consentito solo mediante strumenti, reti, procedure e canali autorizzati. Per i collegamenti da remoto devono essere privilegiate connessioni protette, con autenticazione rafforzata e misure di verifica dell'integrità del dispositivo utilizzato.

Nello svolgimento dell'attività in modalità agile o da remoto, l'utente deve evitare l'utilizzo di reti insicure prive di adeguata protezione, nonché impedire la visione di informazioni da parte di soggetti non autorizzati. È fatto divieto di utilizzare account personali, archivi privati o servizi non autorizzati per la gestione di attività istituzionali.

Posta elettronica

La posta elettronica istituzionale costituisce strumento di lavoro e deve essere utilizzata esclusivamente per finalità di servizio, salvo eventuali usi occasionali consentiti da specifiche disposizioni interne. I messaggi devono essere gestiti con diligenza, verificando il mittente, la coerenza del contenuto, la presenza di allegati inattesi e l'eventuale anomalia di link o richieste di dati.

I sistemi di posta sono configurati secondo criteri di minimizzazione dei dati trattati. La raccolta e conservazione dei metadati di posta elettronica avviene per tempi strettamente necessari al funzionamento, alla sicurezza e alla continuità del servizio, in coerenza con il documento di indirizzo del Garante del 6 giugno 2024 e con le ulteriori valutazioni organizzative e giuridiche dell'Ente.

Procedura da adottare in caso di cessazione del rapporto di lavoro: la prima settimana dopo la cessazione la mail viene bloccata in entrata ed uscita, al dipendente è consentita la sola lettura. In questo periodo la casella di posta elettronica risponde automaticamente "Questa email non è più attiva. Per qualunque comunicazione scrivere a segreteria@esu.vr.it". Trascorsa la settimana l'utente viene cancellato, viene mantenuto il backup del contenuto della casella email e i relativi metadati. Successivamente viene cancellato tutto, metadati compresi.

Non è consentita la lettura sistematica del contenuto dei messaggi di posta da parte dell'Ente. Eventuali accessi a caselle o contenuti devono avvenire solo nei casi consentiti, secondo procedure formalizzate, motivate, proporzionate e adeguatamente documentate.

Navigazione internet e servizi online

La navigazione internet deve essere coerente con le finalità istituzionali e con le esigenze di servizio. L'Ente può adottare sistemi di filtraggio, protezione e registrazione tecnica finalizzati alla sicurezza, alla prevenzione di malware, al contenimento di traffico anomalo e alla tutela dell'infrastruttura.

I log di navigazione non devono essere utilizzati per forme di controllo generalizzato dell'attività lavorativa, ma solo nei limiti consentiti dalla legge, sulla base di finalità determinate e con adeguate garanzie di proporzionalità, necessità e trasparenza.

Cloud, piattaforme collaborative e servizi di terzi

L'utilizzo di servizi cloud, piattaforme di collaborazione, sistemi di archiviazione esterna, videoconferenza o messaggistica è consentito esclusivamente se autorizzato dall'Ente. L'autorizzazione presuppone la verifica di adeguate misure contrattuali, organizzative e tecniche, nonché della coerenza con la disciplina sul trattamento dei dati personali e con i requisiti di sicurezza applicabili.

È vietato caricare, sincronizzare o condividere documenti dell'Ente tramite account personali o servizi non autorizzati. Ogni integrazione tra sistemi interni e servizi di terzi deve essere previamente valutata dalle strutture competenti.

Supporti rimovibili e periferiche

L'uso di supporti rimovibili, memorie esterne, periferiche di archiviazione o dispositivi personali è consentito solo se autorizzato e tecnicamente controllato. Ove ammesso, tali strumenti devono essere sottoposti a verifica di sicurezza e utilizzati in conformità alle misure predisposte dall'Ente.

I supporti contenenti dati dell'Ente devono essere custoditi con particolare diligenza, cifrati ove necessario e, in caso di dismissione, sottoposti a cancellazione sicura o distruzione controllata.

Gestione documentale e conservazione

I documenti e i dati di lavoro devono essere salvati negli spazi istituzionali autorizzati, secondo le regole organizzative dell'Ente e le eventuali policy di conservazione e backup. Non è ammessa la conservazione stabile di documentazione istituzionale in aree locali non presidiate, su dispositivi personali o su repository non autorizzati.

La conservazione di log, metadati, backup e altri dati tecnici deve essere disciplinata da specifiche policy interne che indichino finalità, basi giuridiche, tempi di conservazione, soggetti autorizzati all'accesso e misure di sicurezza applicate.

Controlli tecnici e verifiche

L'Ente può effettuare verifiche tecniche sugli strumenti assegnati e sui sistemi utilizzati per finalità di sicurezza, manutenzione, continuità operativa, prevenzione degli incidenti, protezione del

patrimonio informativo e accertamento di anomalie. Tali verifiche devono essere svolte nel rispetto della normativa applicabile, con modalità non eccedenti rispetto alle finalità perseguite.

I controlli devono essere preferibilmente effettuati su dati aggregati o tecnici e, solo ove strettamente necessario, mediante verifiche individuali supportate da adeguata motivazione, tracciabilità dell'attività svolta e rispetto delle garanzie applicabili.

Incidenti di sicurezza e data breach

Ogni utente è tenuto a segnalare senza ritardo eventi anomali, virus, phishing, accessi non autorizzati, perdita di dati, invio errato di informazioni, smarrimento di dispositivi o altri eventi che possano determinare un incidente di sicurezza o una violazione di dati personali. La segnalazione deve avvenire mediante i canali interni definiti dall'Ente.

Le strutture competenti devono registrare l'evento, valutarne l'impatto, attivare le misure di contenimento, documentare le azioni intraprese e, nei casi previsti, avviare la procedura di gestione del data breach secondo quanto previsto dall'ultima versione della procedura di "Data Breach" approvata e aggiornata al 20.04.2026.

Amministratori di sistema e utenze privilegiate

Le utenze privilegiate devono essere attribuite esclusivamente a soggetti espressamente autorizzati e per il tempo strettamente necessario allo svolgimento delle relative funzioni. Gli accessi amministrativi devono essere tracciati, verificabili e soggetti a controlli periodici.

Le attività degli amministratori di sistema devono essere gestite secondo procedure interne formalizzate, con chiara attribuzione dei ruoli, dei poteri e delle responsabilità, nel rispetto della disciplina applicabile.

Formazione e consapevolezza

L'Ente promuove attività periodiche di informazione, formazione e aggiornamento in materia di sicurezza informatica, protezione dei dati personali, corretto utilizzo degli strumenti digitali e prevenzione dei rischi cyber. I destinatari sono tenuti a partecipare alle iniziative formative obbligatorie previste dall'organizzazione.

Aggiornamento dell'allegato

Il presente allegato è soggetto a revisione periodica, anche parziale, per effetto di modifiche normative, organizzative o tecnologiche, nonché in esito a incidenti, audit, valutazione del rischio o aggiornamenti delle policy interne