AREA A1 - SERVIZI ISTITUZIONALI, PATRIMONIO, INNOVAZIONE E TECNOLOGIA COMUNALE
Servizio: Servizio Segreteria del Sindaco, trasparenza, progetti e finanziamenti speciali, innovazione e tecnologia comunale
Ufficio: Ufficio SITEC e Trasparenza

N° Prop. 1045 del 12/12/2025

DETERMINAZIONE N. 934 del 16/12/2025

OGGETTO: **AREA A1 – SITEC E TRASPARENZA – APPROVAZIONE STATO AVANZAMENTO LAVORI DELLA SOCIETÀ IN HOUSE IN.VA. S.P.A. INERENTE AI SERVIZI DI SUPPORTO E CONDUZIONE PER LA REALIZZAZIONE DEL PROGETTO "POTENZIAMENTO DELLA RESILIENZA CYBER PER IL COMUNE DI AOSTA" NELL'AMBITO DELL'AVVISO PUBBLICO PER LA REALIZZAZIONE DEGLI INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER-PA A VALERE SUL PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5 –- FINANZIATO DALL'UNIONE EUROPEA - NEXT GENERATION EU -- CUP C66G24000050006 – CIG B7346A01D1 – INDIVIDUAZIONE RESPONSABILI DELL'ISTRUTTORIA E RICHIESTA VARIAZIONE ESIGIBILITÀ POSTICIPATA CON CORRELATA REIMPUTAZIONE DI ACCERTAMENTO ED IMPEGNO**

IL DIRIGENTE

Premesso che:

- in data 26 febbraio 2024 l'Agenzia per la Cybersicurezza Nazionale (di seguito anche ACN) ha promosso l'avviso pubblico n. 08/2024 in qualità di Soggetto attuatore dell'Investimento 1.5 "Cybersecurity" – Missione 1, Componente 1, del PNRR, a titolarità della Presidenza del Consiglio dei Ministri - Dipartimento per la trasformazione digitale, a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5, finanziato dall'Unione Europea – Next Generation EU, per l'attuazione degli investimenti finalizzati alla realizzazione di interventi di potenziamento della resilienza cyber per la Pubblica Amministrazione, rivolto, tra gli altri, ai Comuni capoluogo di Regione, nel quale è previsto che i progetti ammessi a finanziamento dovranno concludersi entro il 31 dicembre 2025;
- il Comune di Aosta ha stabilito di aderire al suddetto avviso con deliberazione della Giunta comunale n. 54 del 28 marzo 2024;

- con le nota prot. n. 30781 del 25 settembre 2024, prot. n. 34059 del 21 ottobre 2024 e prot. n. 250 del 3 gennaio 2025, recepite agli atti in pari date al civ. prot. n. 56544/2024, civ. prot. n. 61448/2024 e civ. prot. n. 309/2025, ACN ha trasmesso rispettivamente le Determine prot. n. 30550 del 23 settembre 2024, prot. n. 33707 del 17 ottobre 2024 e prot. n. 43937 del 31 dicembre 2024, recanti l'approvazione della graduatoria finale a valere sull'Avviso n. 8/2024, con relativi allegati, con particolare riferimento all'allegato A riportante la graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziabili, tra le quali risulta quella del Comune di Aosta denominata "Potenziamento della resilienza Cyber per il Comune di Aosta", per un importo finanziabile pari ad euro 671.000,00;
- il suddetto progetto prevede 5 interventi (Governance e programmazione cyber; Gestione del rischio cyber e della continuità operativa; Gestione e risposta agli incidenti di sicurezza; Gestione delle identità digitali e degli accessi logici; Sicurezza delle applicazioni, dei dati e delle reti), per i quali sono previste due tipologie di intervento (Miglioramento dei processi e dell'organizzazione e Progettazione e sviluppo di nuovi sistemi e tecnologie), due categorie di costo (Acquisizione di servizi e Acquisizione di beni), e le attività come di seguito dettagliato:

Intervento	Tipologia di intervento	Attività
1. Governance e programmazione cyber	B. Miglioramento dei processi e dell'organizzazione	Formalizzare una procedura per la gestione, la revisione e l'aggiornamento periodico dell'inventario degli asset dell'organizzazione che includa processi e procedure da adottare per sistemi client, server, utenze, applicazioni aziendali utilizzate on-premises e cloud e le informazioni minime da censire, durante tutto il loro ciclo di vita.
1. Governance e programmazione cyber	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Implementare soluzioni tecnologiche che permettano il censimento degli asset e delle loro configurazioni all'interno di un inventario e la mappatura dei dati e dei loro flussi tra sistemi (CMDB).
2. Gestione del rischio cyber e della continuità operativa	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare una procedura di Business Impact Analysis (BIA).
3. Gestione e risposta agli incidenti di sicurezza	B. Miglioramento dei processi e dell'organizzazione	Integrare la procedura di gestione e analisi dei log, definita in collaborazione con INVA, prevedendo i processi di raccolta, analisi, conservazione, e protezione per tutti i tipi di log (es: log degli amministratori di sistema, log di accesso ai database, log di sicurezza, etc).

3. Gestione e risposta agli incidenti di sicurezza	B. Miglioramento dei processi e dell'organizzazione	Prevedere l'aggiornamento della procedura già esistente di Disaster Recovery, includendo dei piani di ripristino elaborati specificatamente per l'Ente, e che preveda una fase di aggiornamento degli stessi a seguito di test periodici e/o cambiamenti del contesto dell'organizzazione e/o incidente.
4. Gestione delle identità digitali e degli accessi logici	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare all'interno di uno specifico documento le linee guida relative alla gestione sicura delle utenze. In particolare, il documento dovrà contenere indicazioni circa: le modalità di creazione, modifica, cancellazione e ricertificazione delle utenze; le modalità di assegnazione, modifica, rimozione e ricertificazione dei diritti di accesso. Il documento dovrà anche prevedere la necessità di utilizzare solamente utenze nominative ed univoche e regolare l'accesso da remoto alle risorse.
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare una procedura e/o metodologia per la classificazione, gestione e protezione delle informazioni e delle risorse (IT, IoT e Cloud) in base alla loro criticità in termini di riservatezza, integrità e disponibilità, prevendendo l'aggiornamento a cadenza periodica.
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare, all'interno di uno specifico documento, il processo di gestione delle vulnerabilità. Tale processo deve comprendere una fase di identificazione delle vulnerabilità (in modalità continua o periodica), analisi, valutazione e classificazione e, infine, risoluzione.
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Implementare soluzioni di firewall
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Potenziare la sicurezza delle reti locali interne all'Ente (Sostituzione apparati LAN obsoleti delle 7 sedi dell'Ente e attivazione NAC)
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Potenziare la sicurezza delle postazioni di lavoro (Attivazione EDR centralizzato)

- nell'ambito del suddetto intervento denominato "Sicurezza delle applicazioni, dei dati e delle reti" – tipologia di intervento "Progettazione e sviluppo di nuovi sistemi e tecnologie" – categoria di costo "Acquisizione di beni", sono state previste le attività di implementazione delle soluzioni di firewall e attivazione NAC, per le quali il Comune di Aosta con determinazione dirigenziale n. 168/2025 ha stabilito di aderire dell'Accordo Quadro (AQ) – ID 2367 denominato "Cybersecurity 2 – Prodotti e servizi connessi – LOTTO 2, stipulato da CONSIP S.p.A. ai sensi dell'art. 54, comma 3 del D. Lgs n.

50/2016, e Telecom Italia S.p.A., con sede legale in Milano, Via Gaetano Negri n. 1, P. IVA 00488410010 in qualità di impresa mandataria capogruppo del Raggruppamento Temporaneo di Imprese composto, oltre alla stessa, dal-le mandanti Maticmind S.p.A. con sede legale in Milano, Via Roberto Bracco n.6, P. IVA 05032840968, DGS S.p.A., con sede legale in Roma, Via Paolo Di Dono n. 73, P. IVA 03318271214, e SCAI Solution Group S.p.A., con sede legale in Milano, Viale Monte Nero n.73, P. IVA 05348521005; e con successiva determinazione dirigenziale n. 170/2025 ha approvato il relativo ordine di acquisto per un importo pari ad euro 165.765,95 (Iva inclusa);

- per quel che concerne tutte le altre attività previste nei suddetti interventi progettuali, con deliberazione della Giunta comunale n. 63/2025 è stato stabilito di avvalersi del supporto della società partecipata IN.VA. S.p.A., per un importo massimo pari ad euro 503.982,00 (Iva inclusa), nell'ambito del finanziamento progettuale ammesso, e con determinazione dirigenziale n. 533 del 29 luglio 2025 è stato affidato il servizio in argomento alla società IN.VA. S.p.A. per un importo pari ad euro 413.100,00 (Iva esclusa), e quindi in complessivi 503.982,00 (Iva inclusa), il cui contratto è stato sottoscritto nella forma dell'atto pubblico in data 25 settembre 2025 – numero 14777/2025;
- con la suddetta determinazione dirigenziale n. 533/2025 è stato assunto a favore di IN.VA. S.p.A. di Brissogne (C.F. e Partita IVA 00521690073) l'impegno n. 2061/2025 per l'importo di euro 503.982,00, esigibilità 2025, e l'accertamento n. 726/2025 di pari importo;

Precisato che, ai sensi dell'art. 4 della L. 241/90 e in applicazione del modello organizzativo adottato dal Comune in osservanza del principio di auto-organizzazione amministrativa di cui all'art. 7 del D.lgs. n. 36/2023, nella suddetta determinazione dirigenziale n. 533/2025 il RUP è il sottoscritto Stefano Franco, Segretario generale del Comune di Aosta;

Richiamata la deliberazione della Giunta comunale n. 146/2024 con la quale l'ufficio "SITEC e trasparenza" del Servizio n. 11 "Segreteria del Sindaco, progetti e finanziamenti speciali, trasparenza, innovazione e tecnologia comunale" è stato individuato quale Ufficio della transizione al digitale e struttura per la cybersicurezza del Comune di Aosta;

Ritenuto opportuno nominare, ai sensi dell'art. 5 della L. 241/90, quali responsabili dell'istruttoria in relazione agli stati di avanzamento lavori nell'ambito dell'affidamento in essere con la società IN.VA. S.p.A. (determinazione dirigenziale n. 533/2025 e contratto rep. n. 14777/2025) i dipendenti dell'ufficio "SITEC e trasparenza", quale altresì Ufficio della transizione al digitale e struttura per la cybersicurezza comunale, Andrea Sapinet e

Rinaldo Pesciarelli, in possesso delle competenze richieste per lo svolgimento dei suddetti compiti in relazione ai seguenti interventi progettuali:

Intervento	Tipologia di intervento	Attività	Responsabile istruttoria
1. Governance e programmazione cyber	B. Miglioramento dei processi e dell'organizzazione	Formalizzare una procedura per la gestione, la revisione e l'aggiornamento periodico dell'inventario degli asset dell'organizzazione che includa processi e procedure da adottare per sistemi client, server, utenze, applicazioni aziendali utilizzate on-premises e cloud e le informazioni minime da censire, durante tutto il loro ciclo di vita.	Andrea Sapinet
1. Governance e programmazione cyber	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Implementare soluzioni tecnologiche che permettano il censimento degli asset e delle loro configurazioni all'interno di un inventario e la mappatura dei dati e dei loro flussi tra sistemi (CMDB).	Andrea Sapinet
2. Gestione del rischio cyber e della continuità operativa	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare una procedura di Business Impact Analysis (BIA).	Rinaldo Pesciarelli
3. Gestione e risposta agli incidenti di sicurezza	B. Miglioramento dei processi e dell'organizzazione	Integrare la procedura di gestione e analisi dei log, definita in collaborazione con INVA, prevedendo i processi di raccolta, analisi, conservazione, e protezione per tutti i tipi di log (es: log degli amministratori di sistema, log di accesso ai database, log di sicurezza, etc).	Rinaldo Pesciarelli
3. Gestione e risposta agli incidenti di sicurezza	B. Miglioramento dei processi e dell'organizzazione	Prevedere l'aggiornamento della procedura già esistente di Disaster Recovery, includendo dei piani di ripristino elaborati specificatamente per l'Ente, e che preveda una fase di aggiornamento degli stessi a seguito di test periodici e/o cambiamenti del contesto dell'organizzazione e/o incidente.	Rinaldo Pesciarelli

4. Gestione delle identità digitali e degli accessi logici	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare all'interno di uno specifico documento le linee guida relative alla gestione sicura delle utenze. In particolare, il documento dovrà contenere indicazioni circa: le modalità di creazione, modifica, cancellazione e ricertificazione delle utenze; le modalità di assegnazione, modifica, rimozione e ricertificazione dei diritti di accesso. Il documento dovrà anche prevedere la necessità di utilizzare solamente utenze nominative ed univoche e regolare l'accesso da remoto alle risorse.	Andrea Sapinet
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare una procedura e/o metodologia per la classificazione, gestione e protezione delle informazioni e delle risorse (IT, IoT e Cloud) in base alla loro criticità in termini di riservatezza, integrità e disponibilità, prevendendo l'aggiornamento a cadenza periodica.	Andrea Sapinet
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare, all'interno di uno specifico documento, il processo di gestione delle vulnerabilità. Tale processo deve comprendere una fase di identificazione delle vulnerabilità (in modalità continua o periodica), analisi, valutazione e classificazione e, infine, risoluzione.	Rinaldo Pesciarelli
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Potenziare la sicurezza delle reti locali interne all'Ente (Sostituzione apparati LAN obsoleti delle 7 sedi dell'Ente)	Andrea Sapinet
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Potenziare la sicurezza delle postazioni di lavoro (Attivazione EDR centralizzato)	Rinaldo Pesciarelli

Rilevato che i suddetti Responsabili dell'istruttoria hanno dichiarato l'assenza di conflitto di interesse nell'ambito degli interventi a valere sul PNRR (civ. prot. n. 71407/2025);

Dato atto che:

- IN.VA. S.p.A. ha provveduto con nota civ. prot. n. 72964 dell'11 dicembre 2025 alla trasmissione dello Stato Avanzamento Lavori (SAL) al 30 novembre 2025;

- i responsabili dell'istruttoria, come sopra indicati, previa esecuzione delle opportune verifiche, hanno potuto constatare la correttezza delle specifiche attività indicate, accertando che l'intervento affidato è stato eseguito in adempimento alla pianificazione precedentemente condivisa ed in conformità delle prescrizioni contrattuali e delle indicazioni di cui all'avviso pubblico n. 08/2024, PNRR M1C1I1.5 - Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" ed al progetto "Potenziamento della resilienza Cyber per il Comune di Aosta" ammesso a finanziamento;
- in data 12 dicembre 2025, assunto al civ. prot. n. 73256/2025, il sottoscritto RUP, congiuntamente ai suddetti Responsabili dell'istruttoria, hanno sottoscritto il SAL civ. prot. n. 72964/2025 per accettazione;

Ritenuto pertanto opportuno approvare il SAL in argomento, allegato al presente provvedimento, autorizzando al contempo la relativa fatturazione;

Considerato che:

- il suddetto SAL riporta altresì il dettaglio delle attività che saranno effettuate nel 2026 in conformità al citato contratto rep. n. 14777/2025 nel quale è stata indicata all'art. 9 (Termini di attuazione del progetto, durata e proroghe), la data di scadenza contrattuale del 31 marzo 2026 *"(…) attuale data definita a livello governativo per il completamento dei progetti e degli adempimenti di rendicontazione, salvo proroghe da concordare tra le Parti (…)*", in quanto con nota prot. n. 298821 del 29 luglio 2025, recepita al civ. prot. n. 42227/2025 in pari data, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha trasmesso la determina prot. ACN n. 285155 del 23 luglio 2025 recante la proroga al 31 marzo 2026 dei termini di completamento dei progetti e degli adempimenti di rendicontazione previsti inizialmente al 31 dicembre 2025;
- nella citata determinazione dirigenziale n. 533/2025 l'esigibilità risulta essere di euro 503.982,00 per l'anno 2025;

Si ritiene quindi opportuno richiedere al Servizio finanziario di provvedere alla conseguente variazione di esigibilità dall'anno 2025 all'anno 2026, con la correlata reimputazione dell'impegno di spesa n. 2061/2025, nonché dell'accertamento n. 726/2025, in applicazione dei principi contabili contenuti nel D.lgs. 118/2011, ai sensi dell'art. 175, comma 5-quater, lettera b) del D.lgs. n. 267/2000; come segue:

Impegno	**Importo**	**2025**	**2026**
2061/2025	503.982,00	273.524,10	230.457,90
Accertamento	**Importo**	**2025**	**2026**

726/2025	503.982,00	273.524,10	230.457,90

Rilevato il pieno rispetto, in fase istruttoria e di predisposizione degli atti, delle disposizioni contenute nel Codice di comportamento dei dipendenti pubblici e l'insussistenza, ai sensi dell'art. 16 del D.lgs. n. 36/2023, di conflitto di interesse in capo al firmatario del presente atto, nella sua qualità altresì di RUP, agli altri partecipanti al procedimento e in relazione ai destinatari finali dello stesso;

Richiamati:

- la deliberazione del Consiglio comunale n. 174 del 18 dicembre 2024 con la quale sono stati approvati il Bilancio di previsione per il triennio 2025-2027 e i suoi allegati, tra i quali la Nota di aggiornamento al Documento unico di Programmazione (DUP);
- la deliberazione della Giunta comunale n. 2 del 16 gennaio 2025 avente ad oggetto: "Area A2 - Servizio bilancio. Approvazione del Piano esecutivo di gestione 2025-2027";
- la deliberazione della Giunta comunale n. 10 del 31 gennaio 2025 "Approvazione Piano Integrato attività e organizzazione (PIAO) 2025-2027";
- la deliberazione della Giunta Comunale n. 126 del 23 giugno 2021, avente ad oggetto: "Nuovo assetto organizzativo delle aree e dei servizi dell'Ente";
- il decreto del Sindaco n. 71 del 18 novembre 2025 di attribuzione delle funzioni di gestione dell'Area A1 – Servizi Istituzionali, Patrimonio, Innovazione e Tecnologia comunale attribuite al Segretario Generale del Comune di Aosta;

Considerato che l'adozione del presente provvedimento è di competenza del Dirigente ai sensi dell'art. 56 dello Statuto Comunale e per il combinato della L.R. 22/2010 e della L.R. 54/1998 e successive modifiche ed integrazioni;

D E T E R M I N A

1. di approvare l'allegato Stato Avanzamento Lavori (SAL) in relazione al quinto bimestre dell'anno 2025 delle attività svolte da IN.VA. S.p.A. di Brissogne (C.F. e Partita IVA 00521690073) nell'ambito dell'affidamento di cui alla determinazione dirigenziale n. 533/2025 e contratto rep. n. 14777/2025, controfirmato per accettazione dal sottoscritto RUP e dai Responsabili dell'istruttoria;

2. di autorizzare l'operatore economico IN.VA. S.p.A. di Brissogne (C.F. e Partita IVA 00521690073) all'emissione della fattura relativa ai servizi effettuati per un importo pari ad euro 224.200,08 (Iva esclusa) e quindi euro 273.524,10 (Iva inclusa), precisando che per la stessa devono essere rispettate le "Indicazioni per la corretta fatturazione dei servizi oggetto di rimborso a valere del PNRR – Next Generation EU" di cui al documento denominato "v5.0_Allegato_MOA-13_Template indicazioni fatturazione", già inviato all'operatore economico;

3. di trasmettere il presente provvedimento a IN.VA. S.p.A. di Brissogne (C.F. e Partita IVA 00521690073);

4. di dare atto che, ai sensi dell'art. 4 della L. 241/90 e in applicazione del modello organizzativo adottato dal Comune in osservanza del principio di auto-organizzazione amministrativa di cui all'art. 7 del D.lgs. n. 36/2023, il RUP è il sottoscritto Stefano Franco, Segretario generale del Comune di Aosta;

5. di nominare, ai sensi dell'art. 5 della L. 241/90, quali responsabili dell'istruttoria in relazione agli stati di avanzamento lavori nell'ambito dell'affidamento in essere con la società IN.VA. S.p.A. (determinazione dirigenziale n. 533/2025 e contratto rep. n. 14777/2025) i dipendenti dell'ufficio "SITEC e trasparenza", quale altresì Ufficio della transizione al digitale e struttura per la cybersicurezza comunale ai sensi della deliberazione della Giunta comunale n. 146/2024, Andrea Sapinet e Rinaldo Pesciarelli, in possesso delle competenze richieste per lo svolgimento dei suddetti compiti in relazione ai seguenti interventi progettuali:

Intervento	**Tipologia di intervento**	**Attività**	**Responsabile istruttoria**
1. Governance e programmazione cyber	B. Miglioramento dei processi e dell'organizzazione	Formalizzare una procedura per la gestione, la revisione e l'aggiornamento periodico dell'inventario degli asset dell'organizzazione che includa processi e procedure da adottare per sistemi client, server, utenze, applicazioni aziendali utilizzate on-premises e cloud e le informazioni minime da censire, durante tutto il loro ciclo di vita.	Andrea Sapinet
1. Governance e programmazione cyber	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Implementare soluzioni tecnologiche che permettano il censimento degli asset e delle loro configurazioni all'interno di un inventario e la mappatura dei dati e dei loro flussi tra	Andrea Sapinet

		sistemi (CMDB).	
2. Gestione del rischio cyber e della continuità operativa	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare una procedura di Business Impact Analysis (BIA).	Rinaldo Pesciarelli
3. Gestione e risposta agli incidenti di sicurezza	B. Miglioramento dei processi e dell'organizzazione	Integrare la procedura di gestione e analisi dei log, definita in collaborazione con INVA, prevedendo i processi di raccolta, analisi, conservazione, e protezione per tutti i tipi di log (es: log degli amministratori di sistema, log di accesso ai database, log di sicurezza, etc).	Rinaldo Pesciarelli
3. Gestione e risposta agli incidenti di sicurezza	B. Miglioramento dei processi e dell'organizzazione	Prevedere l'aggiornamento della procedura già esistente di Disaster Recovery, includendo dei piani di ripristino elaborati specificatamente per l'Ente, e che preveda una fase di aggiornamento degli stessi a seguito di test periodici e/o cambiamenti del contesto dell'organizzazione e/o incidente.	Rinaldo Pesciarelli
4. Gestione delle identità digitali e degli accessi logici	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare all'interno di uno specifico documento le linee guida relative alla gestione sicura delle utenze. In particolare, il documento dovrà contenere indicazioni circa: le modalità di creazione, modifica, cancellazione e ricertificazione delle utenze; le modalità di assegnazione, modifica, rimozione e ricertificazione dei diritti di accesso. Il documento dovrà anche prevedere la necessità di utilizzare solamente utenze nominative ed univoche e regolare l'accesso da remoto alle risorse.	Andrea Sapinet
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare una procedura e/o metodologia per la classificazione, gestione e protezione delle informazioni e delle risorse (IT, IoT e Cloud) in base alla loro criticità in termini di riservatezza, integrità e disponibilità, prevendendo l'aggiornamento a cadenza periodica.	Andrea Sapinet

5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare, all'interno di uno specifico documento, il processo di gestione delle vulnerabilità. Tale processo deve comprendere una fase di identificazione delle vulnerabilità (in modalità continua o periodica), analisi, valutazione e classificazione e, infine, risoluzione.	Rinaldo Pesciarelli
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Potenziare la sicurezza delle reti locali interne all'Ente (Sostituzione apparati LAN obsoleti delle 7 sedi dell'Ente)	Andrea Sapinet
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Potenziare la sicurezza delle postazioni di lavoro (Attivazione EDR centralizzato)	Rinaldo Pesciarelli

6. di richiedere al Servizio finanziario di provvedere alla variazione di esigibilità dall'anno 2025 all'anno 2026, con la correlata reimputazione dell'impegno di spesa n. 2061/2025, nonché dell'accertamento n. 726/2025, in applicazione dei principi contabili contenuti nel D.lgs. 118/2011, ai sensi dell'art. 175, comma 5-quater, lettera b) del D.lgs. n. 267/2000, come segue:

Impegno	**Importo**	**2025**	**2026**
2061/2025	503.982,00	273.524,10	230.457,90
Accertamento	**Importo**	**2025**	**2026**
726/2025	503.982,00	273.524,10	230.457,90

7. il sottoscritto RUP con nota civ. prot. n. 35344 del 26 giugno 2025 e i responsabili dell'istruttoria come individuati al precedente punto 5. con nota civ. prot. n. 71407/2025, hanno dichiarato l'assenza di conflitti di interesse nell'ambito degli interventi a valere sul PNRR della procedura in argomento e, quindi, il sottoscritto dichiara di non trovarsi, rispetto al ruolo ricoperto nel suindicato procedimento amministrativo, in alcuna delle situazioni di conflitto di interessi, anche solo potenziale, né in qualità di firmatario del presente atto e di RUP, né in relazione agli altri partecipanti al procedimento e ai destinatari finali dello stesso, tali da ledere l'imparzialità dell'agire dell'amministrazione, ai sensi dell'art. 6 bis L. 241 del 1990, art. 53 d.lgs. 165/2001, art. 7 d.p.r. 62/2013, art. 16 D.lgs. 36/2023 e s.m.i.;

8. di dare atto che sono in capo al RUP:

- anche per mezzo degli Uffici competenti, tutti gli adempimenti derivanti dalla presente determinazione;
- gli adempimenti in materia di comunicazioni e trasparenza di cui agli artt. 20 e 23 del d.lgs. 36/2023, compresa la pubblicazione dell'avviso sui risultati delle procedure di affidamento ai sensi dell'art. 50, comma 9 del D.lgs. n. 36/2023;

9. di dare atto che il presente provvedimento non comporta spesa.

RAGIONERIA: verificati impegno n. 2061/2025 e accertamento n. 726/2025


Il Segretario Generale
FRANCO STEFANO
(firmato digitalmente)