**Contratto collettivo integrativo dell'Università degli studi di Siena, relativo all'impiego di sistemi digitali per l'incremento dei livelli di sicurezza informatica anche nello svolgimento di lavoro da remoto.**

Sottoscritta in data 30 settembre 2024.
***(parere positivo del Collegio dei Revisori dei conti – Verbale n. 13/2024 del 20 settembre 2024, Prot. n. 187197 del 23/09/2024***
***delibera del Consiglio di Amministrazione del 23 settembre 2024)***

Le delegazioni trattanti di Parte Pubblica e di Parte Sindacale (*dette, nel prosieguo, anche "Parti"*), costituite ai sensi degli artt. 8, comma 4 e 81, comma 2 del CCNL 18.1.2024 e successiva Delibera Consiglio di amministrazione del 16.02.2024, integrate, per la parte pubblica, ai soli fini della stipulazione del presente accordo, dal Dirigente dell'Area Sistemi informativi, come da delibera in corso di adozione, e così composte:

**Parte Pubblica:**
Delegata del Rettore alle relazioni sindacali
Direttrice Generale
Dirigente AOSI Pierosario Lomagistro

**Parte sindacale**
FLC-C.G.I.L
C.I.S.L. Scuola

Fed. GILDA UNAMS
S.NA.L.S. CONFSAL
R.S.U.

**Premesso che**

- Agli inizi del mese di maggio 2024, l'Università degli Studi di Siena ha subito un attacco cybercriminale di tipo *ransomware* con conseguente esfiltrazione documentale tramite accessi esterni in VPN;
- Tra le misure di sicurezza in atto precedentemente all'attacco informatico (previste nel documento "Misure minime di sicurezza ICT per le pubbliche amministrazioni" di AgID) e attive in Ateneo, vi sono: (a) il controllo del traffico verso siti malevoli che viene automaticamente bloccato dai *firewall* perimetrali con registrazione della URL di destinazione, del dispositivo di origine del traffico e, se disponibile, dell'utenza attiva al momento del blocco; (b) monitoraggio, analisi blocco degli accessi a indirizzi che abbiano una cattiva reputazione; (c) uso di strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli *host* sia su segnalazione degli utenti che in modo automatico da parte del SIEM. Tale sistema generale di sicurezza è operativo su tutto il traffico generato da qualunque dispositivo attivo sulla Rete di Ateneo.
- A seguito dell'evento e a valle delle operazioni di ripristino dei sistemi, si è reso necessario predisporre e prospettare un programma di interventi tutti finalizzati ad elevare la postura di sicurezza dell'Ateneo e della sua architettura informatica. Il programma dei primi interventi proposti da AOSI è stato approvato dagli Organi (Senato Accademico del 16 luglio 2024, rep. n.126/2024, prot. n. 148834 del 18/07/2024, e del Consiglio di Amministrazione del 26/07/2024, rep. 215/2024, prot. n. 158058 del 29/07/2024) ed è allegato sub. All. 1) al presente accordo;
- In particolare, e per quanto rileva ai fini del presente accordo, l'attacco informatico e le operazioni di messa in sicurezza hanno comportato l'interdizione all'uso dei sistemi in accesso da remoto attraverso collegamento VPN (Virtual Private Network).
  L'accesso alla VPN infatti ha rappresentato, e rappresenta, una delle possibili modalità con le quali rendere la prestazione lavorativa durante il lavoro da remoto, cosicché essa non può

costituire di per sé un parametro utile ai fini della valutazione della prestazione lavorativa stessa. Una VPN è un servizio che crea una connessione sicura e privata su Internet criptando i dati che vengono scambiati e rendendoli inaccessibili a chiunque tenti di spiarli. Il programma di interventi per elevare la postura di sicurezza dell'Ateneo prevede diversi livelli di sicurezza a seconda delle risorse a cui si deve accedere. Al primo livello è previsto l'accesso mediante autenticazione a due fattori. A questo livello sarà possibile accedere alle risorse bibliografiche che l'Ateneo mette a disposizione sulla Rete di Ateneo e al Voip; l'utenza tipica è potenzialmente da individuare nell'intera comunità universitaria che necessita di accedere solo a dette risorse. Un livello di sicurezza maggiore è previsto per coloro che accedono a risorse più "sensibili", quali ad esempio i Desktop virtuali oppure i pc fisici collocati nei locali dell'amministrazione, oppure ancora i file memorizzati sulle cosiddette "cartelle condivise". Per questi accessi, è necessario che sul dispositivo che accede alla Rete sia installato il software Forticlient [redacted] che, oltre a richiedere l'autenticazione e due fattori, consente l'accesso alla VPN solo se il dispositivo su cui è installato risponde ai requisiti di sicurezza richiesti dall'Ateneo come di seguito specificato.

– La scelta del programma di sicurezza [redacted] da rendere a breve operativo (oggetto del presente accordo) e finalizzato a restituire accessibilità da remoto in sicurezza, si è basata sugli esiti di una fase sperimentale, volta esclusivamente a testare il sistema di funzionamento del prodotto e, in nessun modo, al controllo a distanza del personale che lo ha utilizzato a tale scopo. La fase volta a verificare le caratteristiche dell'Agente-Software prima del relativo investimento da parte dell'Ateneo ha coinvolto esclusivamente gli operatori dell'AOSI (n. 11 operatori), chiamati a compiere le più diversificate operazioni (volutamente anche rivolte a forzare il sistema), onde valutare le caratteristiche del prodotto sopra menzionato per la messa in sicurezza della Rete digitale di Ateneo. L'esito positivo della fase di test è stato fatto oggetto di resoconto da parte del Responsabile AOSI in sede di riunione sindacale del 23 luglio 2024.

- In occasione di tale riunione sindacale del 23 luglio 2024, le componenti della RSU e delle OO.SS. hanno chiesto di poter estendere la sperimentazione, su adesione volontaria, in favore degli operatori delle Segreterie Studenti (n. 36 dispositivi registrati per il personale delle segreterie studenti) per agevolare massimamente la loro attività lavorativa durante il periodo estivo, particolarmente delicato per le operazioni di immatricolazione studenti.
- Sui fatti riassunti in premessa sono state puntualmente e periodicamente informate Organizzazioni Sindacali e Rsu, e le soluzioni adottate tengono conto delle istanze da tali Organismi pervenute e delle risultanze condivise nel confronto. Si dà inoltre conto che, a latere, è operativo un tavolo tecnico costituito tra le Parti con la finalità di operare la ricognizione sulle risorse di Ateneo in dotazione al PTA e sulle possibili ottimizzazioni/implementazioni.
- La parte pubblica si è avvalsa delle conoscenze e competenze tecniche della AOSI, il cui Dirigente sottoscrive pertanto il presente Accordo sindacale.

**Stante quanto sopra, e considerato che:**

(A) Per gestire gli accessi alle risorse di Ateneo, la scelta effettuata è nel senso di prevedere due fasce di implementazione del sistema di sicurezza:
   - una di primo livello, presidiata da un sistema di accesso con autenticazione a due fattori e per la quale è sufficiente la presenza di "[redacted] **VPN**" (versione base e a licenza d'uso gratuito, già attualmente in uso). Tale primo livello di sicurezza consente l'accesso, tramite una VPN "limitata", alle sole risorse bibliografiche elettroniche dell'Ateneo. È altresì possibile, mediante lo stesso "[redacted] VPN" rispondere tramite computer, tablet o smartphone alle telefonate degli utenti effettuate verso il numero fisso dell'ufficio.

- una di secondo livello, per consentire l'accesso tramite la VPN al proprio *desktop* virtuale o pc fisico, in cui alla autenticazione a due fattori si aggiunge l'installazione nel pc di uno specifico Agente-Software denominato [redacted]. Tale ipotesi consente anche a coloro che accedono da remoto di collegarsi virtualmente al *desktop* dell'ufficio integrato con il client VoIP associato al proprio numero telefonico dell'ufficio. La connessione VPN viene permessa dopo aver verificato che:

[redacted]

(B) Per il secondo livello di protezione, l'Agente-Software individuato costituisce uno strumento più evoluto di quanto finora in uso, in grado di assicurare una maggiore protezione del "patrimonio digitale e informatico" dell'Ateneo e dell'intero apparato documentale gestito dai destinatari del presente accordo, attraverso il ricorso a sistemi di archiviazione, scambio, detenzione digitale che offrano maggiori garanzie di tutela da attacchi esterni o da rischi di violazione e cybercrimini, e quindi in grado di prevenire quanto più possibile comportamenti e fatti dannosi da parte di terzi. In ragione di tali caratteristiche, tale Agente-Software costituisce uno strumento necessario alla esecuzione della prestazione lavorativa quando si abbia la necessità di accedere da remoto, tramite la VPN di secondo livello, alla Rete di Ateneo.

(C) In relazione al sistema di sicurezza di secondo livello, l'Università degli Studi di Siena ha quindi deciso di incrementare il sistema di efficienza e sicurezza digitale e informatica dell'intera Rete di Ateneo, sia per tutte le apparecchiature che sono in dotazione ai destinatari del presente accordo (come pc portatili usati da remoto), sia per quelle che, anche se di proprietà personale, siano usate da lavoratori e lavoratrici per l'esecuzione della prestazione lavorativa da remoto, secondo gli accordi stipulati individualmente, qualora per l'esecuzione stessa sia necessario l'accesso alla VPN di secondo livello.

(D) L'Università degli Studi di Siena estenderà o comunque prevederà l'utilizzo di analoghi sistemi di sicurezza informatica e digitale di secondo livello anche nei riguardi di tutto quel personale di Ateneo (come il personale docente, i dirigenti), come ad altri soggetti esterni, che, a vario titolo, necessitino di accedere alla Rete tramite connessione VPN di secondo livello e non direttamente rientranti nel campo di applicazione del presente accordo.

(E) L'Università degli Studi di Siena ha intenzione di utilizzare l'Agente-Software [redacted] a tutela di patrimonio, beni, archivi, risorse, documenti e tutto quanto in proprietà o gestione digitale e informatica dell'Ateneo, 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.

(F) L'Agente-Software [redacted] per le modalità e le funzioni per le quali viene usato non rientra strettamente nelle previsioni dell'art. 4, comma 1, della l. n. 300/70 e, piuttosto, costituisce uno strumento di lavoro tale per cui trova applicazione la fattispecie di cui al secondo comma dell'art. 4 della l. n. 300/70. Ritenuto, per maggiore trasparenza e condivisione con personale, RSU e OO.SS., ciononostante opportuno addivenire ad un accordo che possa anche valere, a tutti gli effetti, ai sensi dell'art. 4 comma 1, l. 300/70, in virtù del quale: "*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 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 (...) 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.*", le parti addivengono alla presente intesa.

(G) L'art. 51 del D. Lgs. n. 165/2001, al comma 2, prevede che "*La legge 20 maggio 1970, n. 300, e successive modifiche e integrazioni, si applica alle pubbliche amministrazioni a prescindere dal numero dei dipendenti*".

**Tutto ciò premesso e considerato,**
**le Parti Si accordano e convengono quanto segue in ordine all'impiego,**
**ex art. 4, L. n. 300/1970, di sistemi utili a eseguire la prestazione lavorativa e in grado di garantire una maggiore sicurezza informatica dell'intera Rete di Ateneo**

1. Le premesse e i *considerata* costituiscono parte fondamentale e integrante il presente Accordo;
2. L'Università degli Studi di Siena intende avvalersi di [redacted] come indicato in premessa e la cui scheda tecnica è allegata al presente Accordo (All. 4), al solo ed esclusivo scopo:
    a. di tutelare la riservatezza di tutti i dati di cui, a qualunque titolo, è in possesso l'Ateneo; di tutelare l'integrità delle proprie Reti informatiche; di garantire la corretta operatività dei sistemi informatici di Ateneo. Il tutto, con particolare riguardo ai rischi o attacchi informatici esterni e per la tutela da cybercrimini o attacchi informatici;
    b. di fornire un supporto a lavoratori e lavoratrici che prestano attività lavorativa da remoto tramite uso della VPN di secondo livello, consentendo loro di avere sempre a disposizione – installando l'Agente-Software nell'apparecchio digitale usato per rendere la prestazione lavorativa – un sistema in grado di verificare autonomamente se l'apparecchio usato è conforme alle misure minime di sicurezza previste dalla normativa vigente e dal presente accordo.
3. A tal fine, in relazione al precedente punto 2, trattandosi di un Software necessario a rendere la prestazione lavorativa o comunque necessario, secondo il principio di minimizzazione, a verificare la presenza dei requisiti minimi di sicurezza indispensabili per rendere una prestazione lavorativa in sicurezza e nell'adempimento degli accordi stabiliti nell'ambito degli accordi individuali per il lavoro da remoto, l'installazione di tale Agente-Software dovrà avvenire da parte di coloro la cui prestazione lavorativa si svolga in modalità remota e quindi con uso di pc non collegati direttamente alla Rete di Ateneo, che abbiano necessità di accedere al proprio *desktop* virtuale o pc fisico (quindi al secondo livello di sicurezza di cui al precedente *Considerando* (A)).
4. Nei casi previsti dal precedente punto 3, ciascun lavoratore o lavoratrice interessato/a è tenuto/a a presentare apposita richiesta di abilitazione all'accesso in VPN di secondo livello mediante la compilazione di un apposito modulo (cfr. All. 2) contenente la dichiarazione del lavoratore/lavoratrice con cui si impegna a scaricare l'Agente-software di sicurezza informatica indicato nel presente accordo sindacale. Tale modulo andrà dall'interessato consegnato al Responsabile di struttura affinché confermi che il/la richiedente ha necessità di accesso alla VPN di secondo livello per l'effettuazione della prestazione lavorativa; dopo di che, il Responsabile trasmetterà ai tecnici informatici di riferimento le richieste pervenute e costoro potranno così attivare il collegamento alla VPN onde rendere possibile l'esecuzione della prestazione lavorativa anche da remoto. Resta comunque inteso che il Responsabile di struttura potrà autonomamente invitare i propri collaboratori alla compilazione del modulo, in mancanza di richiesta proveniente dagli stessi, laddove costoro svolgano, o possano svolgere, una parte della propria prestazione lavorativa con necessità di accesso alla VPN di secondo livello.

    A tal fine si precisa che, in via di prima applicazione:
    a. Il personale interessato è invitato, nei 10 giorni di tempo dalla sottoscrizione definitiva

del presente accordo sindacale o dall'invito scritto del Responsabile, a presentare richiesta di accreditamento alla VPN di secondo livello;

b. Il personale interessato avrà poi 7 giorni di tempo per scaricare l'Agente-software sullo strumento impiegato per l'esecuzione della prestazione da remoto, decorrente dalla data di invio delle credenziali e/o istruzioni per scaricare l'Agente da parte dei tecnici informatici.

L'autorizzazione ha valenza annuale e si rinnova automaticamente qualora non ricorrano variazioni organizzative; in tali casi, la cessazione della necessità di accedere da remoto tramite VPN viene comunicata via mail dall'interessato/a alla AOSI previo confronto/consenso con il diretto Responsabile. In caso di cessazione nell'utilizzo della VPN o dal servizio, la comunicazione è necessaria al fine di rendere eventualmente trasferibile la licenza.

5. Per tutti coloro che abbiano necessità di accesso alla VPN di secondo livello, il rispetto dei suddetti termini è considerata una condizione necessaria allo svolgimento della prestazione da remoto. La suddetta installazione nei pc personali di lavoratori e lavoratrici che svolgono attività di lavoro da remoto è dunque da considerare una condizione concretamente integrante gli obblighi riportati nella circolare sul lavoro agile (nella parte in cui prevede che "*Il personale è tenuto al rispetto degli obblighi di riservatezza in materia di privacy e di protezione dei dati personali come disposto dal Regolamento dell'Università di Siena "Regolamento sul trattamento dei dati personali in attuazione del Regolamento UE 2016/679 e del D.Lgs. 196/2003"; è inoltre tenuto a rispettare le direttive in materia di sicurezza dell'ambiente di lavoro e di sicurezza informatica. A tal fine in fase di compilazione si dovrà prendere visione delle specifiche informative di Ateneo. Il mancato rispetto degli obblighi sottoscritti nell'accordo individuale può essere motivo di revoca dell'accordo da parte dell'amministrazione*") e negli accordi individuali di lavoro agile, in base ai quali il personale dichiara che "*È stata presa visione dell'Informativa nella quale sono indicati i rischi generali e i rischi specifici connessi alla particolare modalità di esecuzione della prestazione all'esterno della sede di lavoro (DL n. 81/2008), nonché di conformarsi ai requisiti di sicurezza informatica e dei dispositivi personali le cui informative sono disponibili nelle pagine web dell'Ufficio esercizio e tecnologie https://www.uet.unisi.it/sicurezza*".

6. In caso di inerzia del lavoratore o della lavoratrice nella installazione dell'Agente-Software, così come nel caso in cui il sistema interdica l'accesso per la mancanza dei requisiti minimi di sicurezza di cui alle premesse e al successivo punto 7, non sarà quindi consentita l'esecuzione della prestazione da remoto con accesso tramite VPN fino al momento in cui non si provveda nel senso sopra indicato. In tali casi, fatta salva l'interdizione allo svolgimento della prestazione da remoto, il lavoratore e la lavoratrice non possono comunque subire alcun pregiudizio anche di natura disciplinare.
   Ad ogni modo, nel caso in cui al lavoratore o lavoratrice venga temporaneamente interdetto l'accesso mediante VPN successivamente all'accreditamento, costui o costei è invitato/a a verificare tempestivamente con l'Amministrazione e gli uffici competenti le ragioni del mancato accesso in VPN onde poter regolarmente proseguire nella esecuzione della propria prestazione lavorativa da remoto.
7. L'Università degli Studi di Siena è autorizzata ad impiegare l'Agente-Software [redacted] al solo ed esclusivo scopo di verificare che gli apparecchi digitali che accedano alla VPN di secondo livello abbiano:

   [redacted]

   Tale verifica dei requisiti è effettuata solo ed esclusivamente in caso di richiesta di accesso alla VPN e, comunque, a intervalli, durante la connessione alla stessa. Non si tratta quindi di

un controllo che avviene a prescindere, ovvero per il solo fatto di aver istallato [redacted].

In tal modo, la connessione VPN viene permessa dopo aver verificato, da parte del sistema Agente stesso (e non più in autonomia dal singolo lavoratore/lavoratrice, e a propria cura) che la postazione di lavoro rispetti tutti i requisiti indicati nella "Misure minime di sicurezza ICT per le pubbliche amministrazioni" emanate dall'AGID (Agenzia per l'Italia Digitale)".

8. Tutti i dati e le informazioni acquisiti dal Software (tra cui quelli ad esempio relativi ai LOG di accesso alla VPN) saranno detenuti dall'Amministrazione per un massimo di giorni 15, periodo ritenuto una misura minima necessaria ed indispensabile per tenere traccia di eventuali anomalie che potrebbero compromettere la sicurezza della Rete e dell'Ateneo, nel rispetto di quanto indicato anche dall'autorità Garante per la Privacy. In ogni caso, ai sensi dell'art. 5 del GDPR, ", i *dati personali trattati sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*". Per mero tuziorismo, si precisa che l'Amministrazione, *ex* art. 115, d.lgs. 196/2003, quale "*datore di lavoro garantisce il rispetto della personalità e della libertà morale dei lavoratori e delle lavoratrici*".
9. In nessun caso, l'Agente-Software [redacted] potrà essere utilizzato per fini diversi da quelli sopra indicati e in assenza di uno specifico e diverso accordo sindacale. In ogni caso, tutti i dati e le informazioni acquisiti dall'Agente non potranno essere utilizzati per finalità diverse rispetto a quelle stabilite nel presente accordo né potranno essere diffusi o comunicati a terzi, salvo l'adempimento di obblighi di legge in capo al datore di lavoro esplicitamente previsti.
10. In ogni caso l'utilizzo dell'Agente-Software [redacted] e il trattamento dei dati raccolti saranno effettuati tenendo conto dei seguenti principi (e comunque nel rispetto dei principi di cui all'art. 5, Reg. UE 2016/679):
    a. rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, con particolare riferimento alla riservatezza e alla identità e alle abitudini personali;
    b. principio di necessità: i sistemi sono conformati in modo tale da non utilizzare dati personali quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi;
    c. principio di proporzionalità; in ogni caso le caratteristiche del sistema Agente sono definite in modo da comportare un trattamento dei soli dati pertinenti e non eccedenti rispetto alle finalità perseguite.
11. Tutti i dati raccolti, e per il tempo indicato al punto 8 del presente Accordo, saranno trattati soltanto dall'Università degli Studi di Siena, mentre il fornitore dell'Agente-Software non vi avrà alcun accesso e comunque non li tratterà in nessun modo.
12. L'Agente opererà nel seguente modo:

    [redacted]

    Per quanto riguarda le regole sull'utilizzo dell'Agente-Software [redacted] si fa riferimento al Manuale operativo del sistema Agente (All. 4).
13. Le Parti si danno atto che qualora vengano apportate modifiche e/o integrazioni che non alterino in modo significativo l'ambito di operatività del sistema Agente-Software [redacted], in relazione alle tutele contenute nel presente Accordo, l'Amministrazione potrà limitarsi a fornire la relativa informativa preventiva a RSU e OO.SS. Le Parti convengono di verificare congiuntamente lo stato di attuazione dell'Accordo nonché di condividere, al bisogno, eventuali specifiche problematiche legate alla sicurezza.
14. Per quanto riguarda il trattamento dei dati personali relativo all'utilizzo dell'Agente-Software [redacted], che avverrà in conformità alle disposizioni dell'art. 4 e delle

altre disposizioni della l. 300/1970 (stat. lav.), del Reg. UE 2016/679 (GDPR), del Codice in materia di protezione dei dati personali di cui al D. Lgs n. 196/2003 e ss. mod. e int., nonché degli inerenti provvedimenti ed atti interpretativi e di indirizzo e della legislazione in materia applicabile, si fa riferimento all'informativa agli interessati (da fornire prima dell'inizio del trattamento) e al Regolamento sul trattamento dei dati personali di Ateneo (All. 3), agli atti del presente accordo.

15. Il presente accordo riguarda l'acquisto di licenze dell'Agente-Software, a spese dell'Amministrazione, per tutte le macchine di proprietà dell'Amministrazione impiegate per l'accesso alla VPN di secondo livello non direttamente collegate alla Rete di Ateneo e comunque per quelle apparecchiature informatiche che i lavoratori e le lavoratrici utilizzeranno per la prestazione da remoto, quand'anche di loro proprietà. In ogni caso, per l'installazione negli apparecchi digitali utilizzati nel lavoro da remoto, sarà cura delle singole unità di personale provvedere entro i termini indicati al precedente punto 4. L'Università degli Studi di Siena assicura al riguardo che non vi sarà alcun controllo sulle attività svolte da remoto da parte dei lavoratori e delle lavoratrici e sul contenuto delle apparecchiature utilizzate per l'esecuzione della prestazione lavorativa.
16. Il personale riceverà apposita informativa sulle modalità di installazione nei termini e secondo le modalità indicate al punto 4. L'accordo si applicherà tuttavia anche a tutte le apparecchiature che negli anni a venire, fino alla modifica del presente Accordo, sia necessario munire del sistema Agente qui descritto in ragione delle modalità di relativo utilizzo.
17. A tale fine, le modalità previste all'art. 4 del presente accordo integrano i contenuti degli accordi individuali sottoscritti, ed il loro rispetto è necessario ai fini della autorizzazione al lavoro da remoto in VPN di secondo livello.
18. L'Accordo, approvato in sede sindacale, è stato sottoposto all'approvazione del Consiglio di Amministrazione nella seduta del 23/09/2024, previa acquisizione del previsto parere da parte del Collegio dei Revisori dei Conti con verbale n. 13/2024 del 20/09/2024 sulla compatibilità dei costi della contrattazione integrativa con i vincoli di bilancio e quelli derivanti dall'applicazione delle norme di legge, ai sensi dell'art. 40-bis del decreto legislativo n. 165/2001.

Letto, approvato e sottoscritto.

**PER L'AMMINISTRAZIONE:**

PER IL RETTORE, La delegata alle Relazioni sindacali, Prof.ssa Lara LAZZERONI

LA DIRETTRICE GENERALE, Dott.ssa Beatrice SASSI

Il DIRIGENTE-Responsabile AOSI, Dott. Pierosario LOMAGISTRO

**PER LE OO.SS.:**

FLC-C.G.I.L

C.I.S.L. Scuola

Fed. GILDA UNAMS

S.NA.L.S. CONFSAL

LA RAPPRESENTANZA SINDACALE UNITARIA

**Allegati:**

(1) Programma interventi informatici approvati dal Senato Accademico del 16 luglio 2024, rep. n.126/2024, prot. n. 148834 del 18/07/2024, e dal Consiglio di Amministrazione del 26/07/2024, rep. 215/2024, prot. n. 158058 del 29/07/2024
(2) Modulo di abilitazione accesso alla VPN di secondo livello.
(3) Regolamento sul trattamento dei dati personali di Ateneo;
(4) Manuale operativo del sistema Agente e/o altre indicazioni tecniche di funzionamento