**PROTOCOLLO DI INTESA**

**tra**

**REGIONE UMBRIA**

**UMBRIA DIGITALE S.c.ar.l.**

**e**

**UNIVERSITA' DEGLI STUDI DI PERUGIA**

**per la costituzione di un**

**Centro di Eccellenza Regionale sulla Cyber Knowledge per le PMI e la Pubblica Amministrazione**

Premesso che

1. le amministrazioni pubbliche, ai sensi dell'art.15, comma l, della legge 7 agosto 1990, n. 241 e successive modifiche e integrazioni, possono concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune;
2. il D.lgs 50 del 18 aprile 2016 ha riordinato la disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture;
3. la L.R. n. 9 del 29 aprile 2014 "Norme in materia di sviluppo della società dell'informazione e riordino della filiera ICT (*Information and Communication Technology*) regionale." prevede:
   - l'utilizzo del Piano digitale regionale triennale (PDRT) come strumento per individuare missioni, programmi ed interventi attuativi utili a favorire lo sviluppo della società dell'informazione nel territorio umbro;
   - la costituzione del Sistema informativo regionale dell'Umbria (SIRU) quale complesso integrato di procedure, basi di dati e servizi infrastrutturali, telematici ed applicativi per il tramite del Data center regionale unitario (DCRU) che ne è l'infrastruttura abilitante;
   - la collocazione nel DCRU di tutti i sistemi server della Regione, delle Agenzie regionali, delle Aziende sanitarie e ospedaliere, oltre a quelli degli enti locali sulla base di specifici accordi attuativi;
   - la costituzione di Umbria Digitale S.c.ar.l. in conformità al modello comunitario dell'*in house providing*, con lo scopo di erogare, secondo quanto previsto nel PDRT, servizi di interesse generale per lo sviluppo e la gestione della rete pubblica regionale (art. 6 - L.R. 31/2013), dei servizi infrastrutturali della *Community Network dell'Umbria* (art. 10 - L.R. 8/2011) e del DCRU;
4. la DGR n. 829 del 7 luglio 2014 "Programma trasversale consolidamento del data center regionale unitario, sicurezza (continuità operativa e *disaster recovery*) e razionalizzazione dell'infrastruttura digitale dell'Umbria: adozione." approva il "Piano di razionalizzazione dell'Infrastruttura digitale dell'Umbria" (PRID) così come previsto dall'art. 19, comma 2, della L.R. 9/2014;
5. la DGR n. 1778 del 22 dicembre 2014 "Disciplinare per l'attuazione della legge regionale n.9/2014. Approvazione." approva il disciplinare, successivamente pubblicato nel Supplemento ordinario n. 3 al B.U.R. n. 14 dell'11 marzo 2015;

6. la D.G.R. n. 155 del 20 febbraio 2017 “Linee guida strategiche per lo sviluppo della Società dell'Informazione (LGSI) per la legislatura 2015-2020. Adozione proposta ex art. 3, c. 1, L.R. n. 9/2014” definisce le linee guida di cui alla legge regionale n. 9/2014, successivamente approvate con deliberazione n. 213 del 28 novembre 2017 dell'Assemblea legislativa regionale;
7. il POR FESR 2014-2020 della Regione Umbria è stato approvato dalla Commissione EU con Decisione C (2015) 929 del 12/02/2015 e con la conseguente DGR n.184/2015 di presa d'atto della Giunta Regionale;
8. l’Agenzia per l’Italia Digitale ha emanato le “Misure minime per la sicurezza ICT delle pubbliche amministrazioni” (Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015) e, come indicato nel “Piano triennale per l’informatica nella Pubblica Amministrazione 2019-2021” AgID, emanerà le “Linee guida di sicurezza cibernetica per le PA” entro dicembre 2019;
9. il regolamento generale sulla protezione dei dati (GDPR), regolamento (UE) n. 2016/679 adottato il 27 aprile 2016, pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016, entrato in vigore il 25 maggio dello stesso anno è operativo a partire dal 25 maggio 2018;
10. la Regione Umbria ha realizzato e messo a disposizione delle pubbliche amministrazioni umbre il data center regionale DCRU, progettato secondo i migliori standard internazionali, attraverso il quale vengono erogati servizi applicativi per la Regione Umbria e gli enti del territorio;
11. è stato individuato nel PDRT il progetto PRJ-1505 denominato “CERT-PAT”, da finanziare con fondi POR-FESR 2014-2020, che dovrà essere realizzato da Umbria Digitale, per l’istituzione del CERT territoriale umbro al fine di supportare le Pubbliche Amministrazioni Locali (PAL) del territorio per le esigenze specifiche di sicurezza e veicolare l’implementazione sul territorio regionale di regole e modelli organizzativi nazionali in coordinamento continuo col CERT-PA.

Vista la Comunicazione della Commissione europea COM (2010) 245 del 26.08.2010 2010 su “*Un’agenda digitale europea”*;

Vista la Comunicazione della Commissione europea COM (2015) 192 su “*Strategia per il mercato unico digitale europeo”;*

Vista la Comunicazione della Commissione europea COM (2016) 178 del 19.4.2016 su *Iniziativa europea per il cloud computing. Costruire una economica competitiva dei dati e della conoscenza in Europa*;

Vista la Comunicazione della Commissione europea COM (2016) 180 del 19.4.2016 su *Digitalizzazione dell’industria europea. Cogliere appieno i vantaggi di un mercato unico digitale*

Vista la Comunicazione della Commissione europea COM (2017) 228, del 10.5.2017 su *Revisione intermedia dell’attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti* al cui punto 3.3 che prevede di *promuovere la realizzazione di ecosistemi informatici affidabili: affrontare insieme le sfide della sicurezza informatica*;

Vista la risoluzione del Parlamento europeo dell’1.6.2017 sulla *digitalizzazione dell’industria europea*;

Considerato inoltre che:

1. il consolidamento dei processi di digitalizzazione diffuso e massivo che sta investendo le imprese e le pubbliche amministrazioni, e la tendenza crescente verso l'introduzione di tecnologie di cybersecurity, di intelligenza artificiale e di gestione ed acquisizione dei dati, pongono nuove sfide, in termini di valutazione degli impatti organizzativi, di processo e normativi. Si pensi, solo a titolo esemplificativo, agli *health information system* collegati ai servizi sanitari, in cui l'acquisizione massiva di dati altamente sensibili presenta l'esigenza di analizzarli, elaborarli e proteggerli tramite algoritmi matematici e informatici, offrendo opportunità di ricerche avanzate.
2. per rispondere a queste sfide, un numero crescente di istituzioni ha sentito l'esigenza di creare strutture di raccordo, centri di competenze e osservatori (quali ad esempio quali ad esempio l'Osservatorio "Cyber Knowledge and Security Awareness" di ABI) strutture regionali sulle nuove tecnologiecon l'obiettivo di supportare i responsabili dell'Information Governance nell'analisi e nella comprensione dei diversi aspetti legati ai processi di gestione delle informazioni e alle relative tecnologie di supporto, sia in termini di miglioramento qualitativo dei servizi che in termini di impatti normativi e di sicurezza.

Ritenuto di interesse comune la promozione della costituzione, da parte degli organismi di ricerca presenti sul territorio regionale, di un **Centro di Eccellenza Regionale sulla Cyber Knowledge** orientato alla diffusione e al trasferimento di conoscenze sulle principali tendenze di cambiamento normative, tecnologiche e di contesto nel settore della sicurezza informatica, dell' intelligenza artificiale, dell' analisi ed elaborazione dei dati e delle applicazioni digitali nei processi produttivi del sistema delle imprese e della Pubblica Amministrazione;

Ritenuto pertanto opportuno perseguire le seguenti finalità:

- mettere a disposizione delle imprese e delle pubbliche amministrazioni il sistema delle competenze e delle infrastrutture di ricerca;
- valorizzare anche a livello nazionale ed europeo il sistema di competenze regionale in materia di intelligenza artificiale, sicurezza informatica, di acquisizione, analisi ed elaborazione dei dati e dei processi di digitalizzazione delle informazioni;
- condividere le attività di divulgazione che il Centro potrà attivare per favorire e promuovere la conoscenza delle problematiche e delle soluzioni connesse al tema della cyber knowledge nell'ambito dei processi digitali;

individuando gli impegni programmatici di competenza dei sottoscrittori;

TUTTO CIO' PREMESSO

SI CONVIENE QUANTO SEGUE

ART. 1
Premesse

Le premesse fanno parte integrante del presente protocollo di intesa e costituisce il presupposto su cui si fonda il consenso tra le parti per realizzare una attività condivisa finalizzata alla costituzione di un **Centro di Eccellenza Regionale sulla Cyber knowledge**

denominato **CERC**, di seguito Centro, come forma di coordinamento tra i sottoscrittori del presente protocollo di intesa.

ART. 2
Impegni della Regione Umbria

La Regione, nel quadro degli strumenti di programmazione, si impegna a promuovere, a seguito di suo esame, le attività del Centro contenute nel Programma di cui al successivo art.3, mediante:

a. attività di interfaccia collaborativa con il Centro, per azioni di divulgazione delle problematiche e delle soluzioni sulla Cyber Knowledge a favore delle imprese e delle pubbliche amministrazioni, in particolare riguardo all'impatto della introduzione nei processi produttivi delle imprese e delle pubbliche amministrazioni della tecnologia di cybersecurity, di intelligenza artificiale e di acquisizione, analisi ed elaborazione dei dati relativamente alla ottimizzazione dei processi e miglioramento della qualità dei servizi/processi;
b. individuazione di uno o più sedi operative, ove realizzare attività specializzate a supporto delle imprese e delle pubbliche amministrazioni;
c. azioni di supporto all'attivazione di scambi di buone pratiche e attività di collaborazione fra i soggetti firmatari e istituzioni di ricerca, imprese e amministrazioni a scala nazionale e internazionale;
d. attivazione di accordi di collaborazione scientifica per la realizzazione di studi e approfondimenti sul tema della cyber knowledge, sulle potenziali aree di applicazione in Umbria e sui fabbisogni delle imprese, degli organismi di ricerca e delle pubbliche amministrazioni;
e. valorizzazione e promozione delle competenze presenti in Umbria sulla Cyber knowledge.

ART. 3
Impegni dell'Università e di Umbria Digitale

L'Università ed Umbria Digitale si rendono disponibili, su richiesta di Regione Umbria, ad elaborare congiuntamente una proposta operativa di costituzione del Centro, nel rispetto dei rispettivi ordinamenti.

L'Università ed Umbria Digitale costituiranno un Team di lavoro composto da tecnici provenienti da entrambe le realtà, che opereranno in modo congiunto e sinergico nell'ambito della cyber knowledge.
Il Team di lavoro provvederà ad erogare servizi alla PAL ed alle PMI Umbre che sostanzialmente possiamo ricondurre a:

- **Servizi in ambito cyber knowledge**
  - **supporto tecnico scientifico** alle imprese, agli organismi di ricerca, alle pubbliche amministrazioni e ai cittadini;
  - **servizi di formazione e comunicazione** per promuovere la cultura della cyber knowledge;
  - **servizi di alfabetizzazione/sensibilizzazione alle tematiche della sicurezza/gestione/interpretazione dei dati**, ovvero servizi consulenziali, ai vari livelli, operativi e decisionali;

    - **predisposizione di progetti** di ricerca e trasferimento da presentare su bandi regionali, nazionali e della Commissione europea;
- **Servizi più specifici in tema di cybersecurity**
    - **servizi di analisi e di indirizzo**, rivolti a fornire supporto agli enti ed alle imprese nella definizione ed adozione di processi di gestione della sicurezza e di strumenti per la valutazione della sicurezza informatica;
    - **servizi proattivi**, costituendo basi informative frutto della raccolta ed elaborazione di dati relativi alla sicurezza informatica, pubblicando bollettini e/o segnalazioni di sicurezza;
    - **servizi reattivi**, per fornire supporto sia nella interpretazione/gestione degli allarmi di sicurezza, che nella gestione e risoluzione degli incidenti di sicurezza all'interno del dominio regionale umbro;
    - **Servizi di protezione** vera e propria, o erogati centralmente a partire dal DCRU, o sulla base di regole di sicurezza conformi alla direttive nazionali;

Più in particolare, Umbria Digitale si impegna a:

- realizzare il progetto "PRJ-1505 – CERT-PAT" già previsto nell'ambito del PDRT 2019, provvedendo, nella redazione degli step progettuali successivi all'affidamento, a rimodulare il mandato progettuale alla luce del coinvolgimento dell'Università;
- rendere disponibili le risorse tecnologiche necessarie e quindi implementare nel DCRU gli strumenti adeguati a supportare l'operatività del Centro, a titolo esemplificativo e non esaustivo si intende:
    - risorse tecnologiche;
    - strumenti software di analisi;
    - pubblicazione di un sito web informativo da realizzare da parte del Team;
    - Help Desk a disposizione degli utenti per segnalazioni e/o richieste di supporto;

l'Università degli studi di Perugia si impegna a:

- offrire di servizi di certificazione;
- individuare possibili percorsi di alta formazione sul tema della cyber knowledge;
- collaborazione con la Regione alla predisposizione di percorsi di formazione ed educazione in materia di cyber knowledge in generale e della cybersecurity più in particolare.

## ART. 4
## Nucleo tecnico di coordinamento

È costituito un Nucleo tecnico di coordinamento composto da n. 1 rappresentante per l'Università, n. 1 rappresentante per Umbria Digitale e n. 1 rappresentate regionale con il compito di verificare e monitorare le attività previste dal presente protocollo di intesa.

## ART. 5
## Proprietà Intellettuale

Le Parti sono vicendevolmente obbligate al vincolo di confidenzialità per quanto concerne le informazioni, i dati, il *know-how*, le notizie che le stesse scambiano durante la vigenza e/o esecuzione del presente Protocollo, ad eccezione di quelle informazioni, dati, notizie e decisioni per le quali la legge o un provvedimento amministrativo o giudiziario imponga un obbligo di comunicazione e/o salvo consenso della Parte da cui tali dati provengono.

Qualsiasi diritto di proprietà intellettuale di cui sia titolare una Parte resterà nella piena esclusività della stessa, ed il relativo uso che dovesse essere consentito alle altre Parti nell'ambito del presente Protocollo non implicherà il riconoscimento di alcuna licenza e/o diritto in capo alle stesse, salvi i casi in cui il trasferimento sia espressamente e previamente previsto.

Qualsiasi diritto di proprietà intellettuale di cui sia titolare una Parte potrà essere utilizzato dalle altre Parti per le attività di cui al presente protocollo solo dietro espresso consenso della Parte proprietaria ed in conformità alle regole indicate da tale Parte definita "titolare".

ART. 6
Trattamento dei dati personali

Le Parti consentono il trattamento dei loro dati personali ai sensi del Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 ("GDPR") e del D.Lgs. 196 del 30 giugno 2003 e s.m.i. ("Codice della Privacy"); gli stessi dati potranno essere inseriti in banche dati, archivi informatici e sistemi telematici solo per fini connessi al presente Protocollo.

Nell'ambito del trattamento dei dati personali connessi all'espletamento delle attività oggetto del Protocollo, le Parti, ciascuna per le rispettive competenze, opereranno nel rispetto delle disposizioni dettate dalle normative sopra citate in qualità di Titolari autonomi.

Le Parti si impegnano reciprocamente, in attuazione degli obblighi di sicurezza imposti dal GDPR, dal D.Lgs. 196/2003 e da ogni altra disposizione legislativa e regolamentare in materia, a custodire i dati personali trattati in modo da evitare rischi di distruzione degli stessi o di accessi a tali dati da parte di soggetti non autorizzati.

ART. 7
Controversie

Per tutte le controversie derivanti dall'interpretazione o dall'esecuzione del presente Protocollo, le Parti procederanno per via amministrativa, dopo aver esperito e senza alcun risultato, un tentativo di bonaria composizione extragiudiziale. Nel caso in cui non si dovesse pervenire ad un accordo, competente per eventuali controversie, è il Foro di Perugia.

Per quanto posso occorrere, restano comunque salve le competenze inderogabili previste dalle applicabili disposizioni di legge.

ART. 8
Registrazione

Il presente Protocollo è soggetto a registrazione solo in caso d'uso ai sensi degli artt. 5, 6 e 39 del D.P.R. n. 131 del 26 aprile 1986 e non è soggetto ad imposta di bollo ai sensi e per lo effetto del D.P.R. 642/72 e successive modifiche ed integrazioni.

Le spese per l'eventuale registrazione sono a carico della Parte richiedente.

Il Protocollo avrà piena efficacia a decorrere dalla data della sua sottoscrizione anche a mezzo di firma digitale ai sensi e nel rispetto del D.P.C.M. del 22 Febbraio 2013, pubblicato sulla G.U. N. 117 del 21 Maggio.

ART. 9
Modifiche ed integrazioni

Eventuali modifiche sostanziali al presente protocollo di intesa potranno essere apportate solo con il consenso unanime dei sottoscrittori.

Eventuali variazioni non sostanziali che si dovessero rendere necessarie in fase di progettazione o di attuazione di quanto previsto potranno essere approvate, senza che ciò determini variazioni al presente protocollo e saranno oggetto dell'esame e approvazione da parte del Dirigente responsabile del procedimento.

ART. 10
Validità del protocollo di intesa

Il presente protocollo ha validità sino al 31.12.2023 a decorrere dalla data di sottoscrizione.

Ciascuna delle Parti avrà la facoltà di recedere dal presente Protocollo, senza oneri o corrispettivi, dandone comunicazione scritta alle altre Parti con un preavviso di almeno 90 (novanta) giorni.

In caso di recesso restano salve le eventuali iniziative già avviate congiuntamente, salvo che le Parti di comune accordo non decidano diversamente

Letto, approvato e sottoscritto

Perugia, ___/___/_____

Per la Regione Umbria _____

Per Umbria Digitale S.c.ar.l. _____

Per l'Università degli Studi di Perugia _____