FONDAZIONE
EDMUND MACH

Allegato C

Predisposto, come stabilito dalla deliberazione del CdA n. 19 di data 26/4/2022, e pubblicato il 1/6/2022

C.16 Procedura

ICT per l'accesso e l'utilizzo dei servizi informatici, telematici e telefonici della rete FEM[1]

(ai sensi dell'art. 1 c. 6 del ROF)

[1] Procedura adottata con disposizione del Presidente n. 3 di data 26/09/2019, con efficacia dal 01/10/2019. Parte integrante della Procedura C. 15 già Regolamento ICT – deliberazione del CdA n. 3 del 09/08/2018.

1. DEFINIZIONI

Ai sensi della presente Procedura, in conformità con il GDPR ed i provvedimenti del Garante, i seguenti termini assumono il significato per ciascuno di essi indicato, a prescindere dall'utilizzo al singolare o al plurale, anche ove utilizzati in parti precedenti di questa Procedura:

i. **Amministratore di sistema**: la persona fisica dedicata alla gestione ed alla manutenzione di impianti di elaborazione o di sue componenti e tutte le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali, quali gli amministratori di basi di dati, di reti informatiche, di apparati di sicurezza e di sistemi *software* complessi, nella misura in cui consentano di intervenire sui dati personali; soggetti che, pur non essendo preposti ordinariamente ad operazioni implicanti una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), possono, nelle loro consuete attività, essere concretamente responsabili di specifiche fasi lavorative comportanti elevate criticità rispetto alla protezione dei dati personali. Vanno considerati a tutti gli effetti alla stregua di trattamenti di dati personali il salvataggio dei dati (*backup/recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione *hardware*, anche quando non consultati "in chiaro" dall'amministratore;

ii. **Autorizzato/autorizzato del trattamento**: persona fisica autorizzata a compiere operazioni di trattamento dati, sulla base dei regolamenti adottati dal Titolare del trattamento e delle istruzioni impartite dal Responsabile del trattamento;

iii. **Comunicazione di dati personali**: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione;

iv. **Contitolare del trattamento**: altra organizzazione che, quale titolare ulteriore del trattamento, determina congiuntamente al Titolare le finalità e i mezzi del trattamento in modo trasparente e mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR;

v. **DataCenter**: La locazione fisica ospitante il complesso delle infrastrutture informatiche e telematiche adibite all'erogazione dei relativi servizi, parte del Sistema ICT;

vi. **Dati aziendali:** i dati e le informazioni trattati nell'ambito delle attività di FEM diversi dai dati personali che rappresentano una proprietà aziendale, patrimonio di FEM.

vii. **Dati biometrici**: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

viii. **Dati genetici**: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla sua fisiologia o salute;

ix. **Dati giudiziari**: dati idonei a rilevare informazioni riguardo provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

x. **Dati identificativi:** dati personali che permettono l'identificazione diretta di una persona fisica;

xi. **Dati particolari:** dati personali di natura sensibile, genetica o biometrica di una persona fisica;

xii. **Dato personale**: qualsiasi informazione che identifica o rende identificabile una persona fisica e che può fornire dettagli sulle sue caratteristiche fisiche, fisiologiche, genetiche o psichiche, sulle sue abitudini, sul suo stile di vita, sulle sue relazioni personali, sul suo stato di salute o sulla sua situazione economica;

xiii. **Dati sensibili**: dati personali idonei a rivelare lo stato di salute (attinenti alla salute fisica o mentale, compresa la prestazione di servizi di assistenza sanitaria) e la vita sessuale, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale di una persona fisica;

xiv. **Diffusione di dati personali**: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

xv. **FEM**: Fondazione Edmund Mach;

xvi. **Garante**: il Garante per la protezione dei dati personali;

xvii. **GDPR**: il Regolamento generale sulla protezione dei dati (UE) 2016/679 - *General Data Protection Regulation*;

xviii. **Interessato**: persona fisica cui si riferiscono i dati personali trattati;

xix. **Procedura**: la presente Procedura ICT per l'accesso e l'utilizzo dei servizi informatici, telematici e telefonici della rete FEM;

xx. **Profilazione**: qualsiasi forma di trattamento automatizzato di dati personali che consiste nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

xxi. **Pseudonimizzazione**: trattamento dei dati personali effettuato in modo tale che tali dati non possano più essere attribuibili ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuibili a una persona fisica identificata o identificabile;

xxii. **Regolamento Accessi**: il Regolamento di gestione sistema controllo degli accessi presso le strutture del complesso edilizio di San Michele all'Adige della Fondazione Edmund Mach (allegato B.20 del ROF-FEM);

xxiii. **Regolamento ICT**: il Regolamento ICT della Fondazione Edmund Mach, approvato con deliberazione n. 3 del 9 febbraio 2018 (allegato B.23 del ROF-FEM);

xxiv. **Responsabile della protezione dei dati o *Data Protection Officer* o DPO**: persona fisica nominata dal Titolare del trattamento che, ai sensi degli artt. 37-39 del succitato GDPR, operando in modo indipendente rispetto all'organizzazione, consiglia il Titolare riguardo obblighi, requisiti ed evoluzione normativa, realizza verifiche interne sulla corretta applicazione delle disposizioni normative e del sistema di gestione *privacy* definite dal Titolare, assistendolo altresì in merito alla valutazione di impatto *privacy* e sull'analisi del rischio. Infine, rappresenta il punto di contatto per interessati e Garante;

xxv. **Responsabile del trattamento**: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato;

xxvi. **Risorse Informatiche**: l'insieme dei dispositivi (computer, notebook, periferiche, ecc.) servizi informatici (software, applicativi, posta elettronica, accesso internet, sistema documentale, ecc.) e infrastrutture di rete (dispositivi attivi e passivi di networking) gestiti dalla RSIC;

xxvii. **RPCA**: la Ripartizione Patrimonio, Contratti e Affari generali della Direzione Generale di FEM;

xxviii. **RSIC**: la Ripartizione Sistemi Informativi e Comunicazione della Direzione Generale di FEM;

xxix. **Sistema ICT**: i sistemi, le dotazioni informatiche e di telecomunicazione di proprietà o nella disponibilità di FEM, nonché i relativi servizi messi a disposizione dalla rete informatica e telematica;

xxx. **Sub-responsabile del trattamento**: persona fisica o giuridica, autorità pubblica, servizio o altro organismo alla quale un Responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento;

xxxi. **Terzi**: clienti, fornitori, consulenti, visitatori, esterni;

xxxii. **Titolare del trattamento o Titolare**: FEM, quale organizzazione nel suo complesso, nella persona del suo Legale Rappresentante che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza;

xxxiii. **Trattamento di dati personali**: qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicata a dati personali, o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'estrazione, la

consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

xxxiv. **Utente**: ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, ogni individuo in possesso di specifiche credenziali di autenticazione con accesso ai sistemi informativi di FEM. Gli Utenti nell'ambito della loro attività e dei loro diritti d'accesso sono nominati quali "Autorizzati del trattamento dei dati" nei limiti dei compiti e delle abilitazioni attribuite;

xxxv. **Violazione di dati personali**: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. SCOPO DI APPLICAZIONE E DESTINATARI

1. Lo scopo della presente Procedura è quello di definire un insieme di *policy* comportamentali a cui i dipendenti, i collaboratori ed eventuali Terzi, che operano FEM, devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni. La Procedura è elaborata in conformità al Regolamento ICT, ne costituisce parte integrante ed è volta a dettagliare le modalità tecnico operative per l'accesso e l'utilizzo del Sistema ICT.
2. La Procedura è realizzata in conformità alle richieste previste dal GDPR costituendone la base per le lettere di nomina e autorizzazione in linea con il GDPR, ed i provvedimenti del Garante.
3. La Procedura si applica ai dipendenti, senza distinzione di ruolo e/o livello, dirigenti, consulenti esterni nonché ai collaboratori di FEM a prescindere dal rapporto contrattuale con la stessa intrattenuto (co.co.co., stagista, tirocinante, dottorando, assignista di ricerca, borsista, ecc.). e a personale o collaboratore di altri enti riconosciuti affiliati a FEM

3. ACCESSO AGLI UFFICI

1. L'accesso agli uffici del Titolare avviene attraverso *badge* e/o chiave personale, esclusivamente da personale autorizzato dal Titolare in base a precise e motivate esigenze di accesso a tali ambienti per finalità lavorative, secondo modalità ed indicazioni riportate nel Regolamento Accessi.
2. I Terzi potranno avere accesso alle aree del Titolare esclusivamente se accompagnati da personale interno.

4. ACCESSO AL DATA CENTER

1. L'accesso ai locali Data Center di FEM è consentito esclusivamente a personale autorizzato ed avviene mediante *badge* personale opportunamente configurato;
2. I Terzi potranno avere accesso al Data Center esclusivamente se accompagnati da personale interno autorizzato all'accesso;
3. Il locale Data Center è dotato di porta di accesso con chiusura e blocco automatico.

5. CUSTODIA DEL BADGE/CHIAVE DI ACCESSO LOCALI

1. Le chiavi /abilitazioni badge di accesso alle aree ed agli uffici sono rilasciate dall'Ufficio tecnico e manutenzione della RPCA a coloro che siano autorizzati da FEM in conformità con il Regolamento Accessi, in base a necessità lavorative mediante procedura connessa alla presenza e durata di un rapporto formalizzato con FEM, memorizzato nei sistemi HCM-HR di FEM.

6. POSTAZIONI DI LAVORO

1. L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi assegnati.
2. La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati (in via esemplificativa e non esaustiva, contenenti particolari sensibili, giudiziari, confidenziali) senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

7. MISURE FISICHE DI CUSTODIA DEI DOCUMENTI E ATTI CARTACEI

1. I dati cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi negli armadi posti nel proprio ufficio. Gli archivi sono ad accesso limitato, per cui è possibile accedervi in caso di necessità per prelevare e riporre i documenti ed i supporti informatici necessari per lo svolgimento delle mansioni lavorative.
2. I documenti dovranno essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi. Gli archivi di documenti e atti contenenti dati personali particolari sensibili o giudiziari dovranno essere custoditi in armadi chiusi a chiave.
3. L'eliminazione fisica di ogni documento cartaceo contenente dati e informazioni aziendali e/o personali deve essere effettuata utilizzando l'apposito elimina-documenti o comunque in una modalità che renda irrecuperabile il documento originale.

8. TRATTAMENTO DEI DATI PERSONALI E AZIENDALI

1. Ogni incaricato è responsabile dei dati e delle informazioni dei quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare tali dati e informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza ed il corretto utilizzo.
2. Il trattamento di qualunque dato e informazione nell'ambito della propria attività lavorativa, deve prevedere da parte del collaboratore incaricato, ogni ragionevole misura per assicurare l'integrità di tali dati e informazioni. I dati e le informazioni potranno essere comunicati a Terzi esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.
3. È vietata la comunicazione all'esterno di dati e informazioni che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale ed alla redditività aziendale o che possano violare i vincoli contrattuali e di legge che concernono le attività di FEM, anche con riferimento ai rapporti di lavoro.
4. È assolutamente vietata la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare, senza espressa autorizzazione della Direzione Generale.
5. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.
6. Si ricorda inoltre che la diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione della presente Procedura, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione nonché come violazione della normativa che regola il rapporto di lavoro.

9 MODALITÀ DI ACCESSO AI SERVIZI EROGATI DALLA RETE FEM

1. L'erogazione delle credenziali di accesso alla rete e servizi ICT di FEM e loro validità avviene mediante procedura connessa alla presenza e durata di un rapporto formalizzato con FEM, memorizzato nei sistemi HCM-HR della stessa.
2. La RSIC garantisce riservatezza ed univocità delle credenziali (Utente-password) associate all'Utente per l'utilizzo dei servizi di rete.
3. Fatte salve specifiche e giustificate esigenze, controfirmate dal Dirigente della struttura richiedente ed autorizzate dalla RSIC, qualsiasi accesso alla rete viene associato ad una persona fisica cui imputare le attività svolte utilizzando le relative credenziali.
4. L'Utente che ha ottenuto l'accesso ai servizi di rete si impegna a:
   a) Rispettare le norme disciplinanti le attività e i servizi che si svolgono nella rete;
   b) Non commettere abusi e a non violare i diritti degli altri utenti e dei terzi;
   c) Assumere la totale responsabilità delle attività svolte tramite la rete stessa;
   d) Conservare ed utilizzare le credenziali fornite (Utente-password) per uso esclusivamente personale ed è responsabile delle attività svolte tramite le stesse;
   e) Mantenere in efficienza e in buono stato la postazione assegnata o concessa in uso, attuando tutto il possibile per proteggere macchinari e *software* da danneggiamenti accidentali o colposi.

10 GESTIONE DELLE CREDENZIALI DI ACCESSO E DELLE *PASSWORD*

1. L'accesso alla rete aziendale attraverso i sistemi informatici può avvenire esclusivamente se preventivamente identificati ed autenticati, previa verifica delle proprie credenziali di accesso costituiti dal *login* e *password*. Le credenziali di autenticazione per l'accesso alla rete e per altri servizi sono inizialmente assegnate dall'Amministratore di sistema, quindi modificate in autonomia dall'Utente.
2. Qualunque variazione delle credenziali di accesso alla rete aziendale/applicazioni/*data base*/archivi/cartelle/risorse dei sistemi dovrà essere concordata ed autorizzata dall'Amministratore di sistema.
3. È necessario prestare la massima attenzione nell'utilizzo, gestione e conservazione delle credenziali necessarie all'accesso dei sistemi informatici. La *policy* per la gestione della *password* deve essere applicata da ogni Utente e si compone dei seguenti criteri:
   a) *Password* strettamente personale;
   b) *Password* di almeno 8 caratteri alfanumerici;
   c) Modifica obbligatoria della password ogni 3 mesi come indicato dal sistema;
   d) Adozione di criteri di complessità tramite l'inserimento nella password di alcuni caratteri speciali ($ # \ /…) eventualmente suggeriti dal sistema in fase di inserimento.
4. L'Utente dovrà attenersi alle seguenti prescrizioni:
   a) La *password* non può essere comunicata a nessun altro Utente o terza parte;
   b) La *password* non deve essere annotata all'interno dell'ufficio o conservata *on-line*;
   c) In caso di dimenticanza e/o ripristino della *password*, dovrà essere inoltrata una richiesta all'Amministratore di sistema.
5. Nell'ambito della gestione delle credenziali di autenticazione e dei profili Utente, è compito dell'Amministratore di sistema:
   a) Verificare la correttezza degli accessi al sistema riportando eventuali abusi;
   b) Verificare periodicamente la coerenza dei profili Utente con le responsabilità/attività assegnate in collaborazione con il Titolare.

11. PERDITA DELLE CONDIZIONI DI AUTORIZZATO O CESSAZIONE DEL RAPPORTO

In caso di perdita delle condizioni di Autorizzato al trattamento o di cessazione del rapporto con FEM, valgono le seguenti regole operative:

a) Le credenziali per l'accesso alla rete ai servizi erogati vengono immediatamente disattivate;
b) La casella di posta elettronica rimane attiva per 1 mese per favorire le attività di comunicazione e termine attività in FEM. Scaduto il primo mese la casella viene disattivata e resa inaccessibile, in attesa di successiva eliminazione. La rimozione dei dati Utente presenti sulle piattaforme *File Server* FEM e Drive-Google FEM, segue le stesse tempistiche indicate per la posta elettronica;
c) Il dirigente responsabile ha facoltà di chiedere il mantenimento della casella di posta elettronica dell'ex dipendente per il periodo strettamente necessario al completamento di quelle attività istituzionali la cui durata si estenda per un periodo successivo alla conclusione del contratto per cui FEM mantenga i diritti di proprietà intellettuale. Detta casella di posta verrà mantenuta attiva, se il caso, solamente per la ricezione dei messaggi e per il loro inoltro ad altra casella di posta;
d) È facoltà di FEM effettuare eventuali operazioni di conservazione di dati o *mail* di carattere professionale di utenti non più appartenenti all'organizzazione. Tali attività sono effettuate dagli Amministratori di Sistema, che potranno pertanto avere accesso, per esclusive ragioni di carattere tecnico.

12. ATTIVITA' DI CONTROLLO

1. Richiamate le disposizioni di cui all'art. 8 del Regolamento ICT ("Controllo"), gli Amministratori di Sistema nell'espletare le attività di controllo, analizzano i *file Log* generati automaticamente da dispositivi preposti al controllo della rete e dei servizi erogati di FEM.

2. I *file Log* analizzati comprendono:
   a) Traffico IP – per analisi del corretto funzionamento del sistema, monitoraggio SLA, controlli di sicurezza: *Log* del traffico IP generato dai dispositivi informatici. Tale *log*, pseudonimizzato, comprende anche dati puntuali di navigazione (url) riferibili all'indirizzo IP interno di provenienza della richiesta;
   b) Accesso alle reti – per analisi del corretto funzionamento del sistema, monitoraggio SLA e controlli di sicurezza: *Log* di accesso alle reti dall'esterno e dall'interno della rete FEM;
   c) Telefonia – per analisi del corretto funzionamento del sistema: *Log* delle chiamate (numero chiamante, numero chiamato, durata).
3. I file di *Log* sono conservati per circa 24 settimane in un sistema accessibile solo dagli amministratori di sistema autorizzati, e non utilizzato normalmente per altre attività di FEM. Tuttavia potranno essere conservati per tempi superiori per giustificate ragioni tecnico/organizzative, per garantire l'esercizio o la difesa di un diritto in sede giudiziarie e in tutti i casi in cui sia richiesto dall'autorità giudiziaria.
4. Sempre in caso di sospetti problemi di sicurezza e di protezione dei dati potrà essere chiesta all'Utente la sua collaborazione nella risoluzione dei problemi.

13 MODALITÀ DI PRESTAZIONE DEI SERVIZI

1. L'erogazione dei servizi di rete e l'accesso alle diverse risorse disponibili avviene mediante accesso a reti diverse a disposizione degli utenti FEM:
   a) **Rete FEM-Intra**: riservata a dispositivi di proprietà di FEM (gestiti centralmente o concessi in gestione autonoma). Erogazione di servizi e piattaforme FEM con accesso cablato e *WiFi*;
   b) **Rete *Guest*:** riservata a dispositivi di proprietà privata (non FEM), per accesso di utenza FEM o utenza ospite. Erogazione del solo servizio di navigazione internet via *WiFi* verso destinazioni esterne alla FEM, previa registrazione dell'utenza (in diverse modalità);
   c) **Rete GARR**: FEM ha stipulato una specifica convenzione con il Consortium della Rete Italiana dell'Università e della Ricerca, che gestisce una rete denominata comunemente "Rete GARR". L'utilizzo dei dispositivi informatici è soggetto al rispetto delle *Acceptable Use Policy* della rete GARR disponibili al seguente *link*: https://www.garr.it/it/regole-di-utilizzo-della-rete-aup. Accesso via *WiFi* servizio GARR-Edu*Roam*, erogazione del solo servizio di navigazione *internet*;
   d) **Rete Strumentale:** riservata a dispositivi e strumenti di laboratorio, analisi e sensoristica. Erogazione limitata di alcuni dei servizi della rete FEM-Intra, tra cui navigazione *internet*, *printer server*, *storage share*. Accesso alla rete è di tipo cablato e *WiFi*;
   e) **Rete DMZ**: riservata a dispositivi *server* FEM, gestiti centralmente che offrono servizi all'esterno.
2. La RSIC in relazione alla propria attività di gestione e manutenzione della rete e dei suoi servizi, si riserva di interrompere i servizi agli utenti con un preavviso adeguato e concordato con il personale addetto dei centri al fine di ridurre al minimo inconvenienti associati all'erogazione di servizi interni ed esterni.
3. La RSIC può interrompere un servizio o un accesso alla rete se rilevi che questo costituisca una palese attuazione di abuso, possa arrecare danno alle sue strutture, ad un altro Utente, o interrompere/ridurre l'operatività e l'efficienza della rete e dei suoi servizi.

14 POSSIBILITÀ DI GESTIONE AUTONOMA DEGLI STRUMENTI INFORMATICI DI PROPRIETÀ DI FEM

1. Su esplicita e motivata richiesta dell'Utente e previa autorizzazione del suo diretto Responsabile, è possibile ottenere la delega della gestione di strumenti informatici di proprietà di FEM (*administrator/root access*).
2. L'Utente, al momento della scelta di questa particolare modalità di utilizzo, dovrà sottoscrivere un documento di richiesta in cui in cui viene designato "Responsabile della gestione autonoma di strumenti informatici di proprietà di FEM", assumendo a suo carico la piena responsabilità circa il rispetto del GDPR nonché circa il rispetto delle norme in tema di diritto d'autore e di altri diritti di proprietà intellettuale, esonerando FEM da ogni e qualsivoglia responsabilità al riguardo.

3. L'Utente richiedente deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate ai fini del rispetto delle norme sopra citate e della riservatezza dei dati di cui FEM è Titolare. FEM si riserva il diritto di revocare le credenziali amministrative, a sua insindacabile discrezione, ove rilevi danni o malfunzionamenti a servizi o strumenti riconducibili alle condotte dell'Utente.
4. L'accesso ai servizi della rete sarà possibile con le stesse regole di accesso alla rete FEM-Intra.
5. La gestione in autonomia implica capacità di gestione e *debug* degli strumenti informatici. Da ciò ne consegue che il supporto del Servizio IT, sarà limitato alla sola parte *hardware* come previsto dalla garanzia, mentre per quello *software*, il supporto si limiterà al ripristino della macchina nella configurazione iniziale standard.
6. Non dovranno essere in alcun modo modificate le configurazioni della rete e del Dominio Microsoft di FEM.
7. Non dovranno essere in alcun modo rimosse o alterate le utenze *administrator* o *root* di FEM necessarie per la gestione e l'aggiornamento dei sistemi.

15 UTILIZZO DI STRUMENTI INFORMATICI PERSONALI IN RETE FEM E ACCESSO AI SERVIZI PER UTENZA OSPITE.

1. Per ragioni connesse alla sicurezza delle infrastrutture e dei dati FEM, l'utilizzo di strumenti informatici personali è consentito con accesso alla sola rete *Guest* via *Wi-Fi*. Il servizio erogato in rete *Guest* è esclusivamente la navigazione *internet* verso destinazioni esterne alla rete FEM. Non è previsto né concedibile l'accesso a risorse interne della rete FEM.
2. Eccezioni alle disposizioni del punto 15.1, potranno essere analizzate ed eventualmente autorizzate dal Responsabile della RSIC e dal Responsabile del richiedente solo in casi di indispensabile necessità e privi di alternativa. In questa particolare circostanza, è fatto obbligo all'Utente, adottare ogni forma di tutela per prevenire possibili infezioni virali o attacchi in rete generati da software malevolo a bordo dello strumento personale.
3. Nel caso di utilizzo di dispositivi personali per utenza ospite, è disponibile un servizio di accesso a rete *Guest* via *Wi-fi* con opportuna procedura di registrazione dell'utenza.
4. I servizi erogati nella rete *Guest* sono soggetti alle attività di controllo di cui al punto 12 della presente Procedura.

16 POSTA ELETTRONICA

1. In relazione all'attività svolta presso FEM, ad ogni Utente può essere concessa in uso una casella di posta nominativa.
2. In ottemperanza alle indicazioni di cui all'art. 5, comma 3 del Regolamento ICT ("Uso del sistema ICT – posta elettronica"), le caselle di posta elettronica date in uso al dipendente sono destinate ad un utilizzo di tipo aziendale per finalità professionali. In quanto tali si segnala che:
   a) Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
   b) Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, *forum*, *social network*, *newsletter* o *mailing-list*, non attinenti l'attività lavorativa;
   c) È vietata la diffusione consapevole e incontrollata di "Catene di Sant'Antonio".
3. Salvo diversa disposizione richiesta dal Dirigente della struttura di appartenenza, attività istituzionali effettuate in rappresentanza di FEM devono avvenire utilizzando caselle di posta elettronica messe a disposizione dalla stessa.
4. In caso di assenza, o in prossimità di cessazione del rapporto con FEM, sono messe a disposizione del dipendente apposite funzioni di sistema che consentono di inviare automaticamente messaggi di risposta ai mittenti. L'uso di queste funzioni è adibito a specificare la data prevista di rientro in servizio e, ove necessario, il nominativo del sostituto o struttura/servizio di riferimento, o indirizzo alternativo in caso di prossima cessazione del rapporto.

5. L'apertura di caselle di posta, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, viene gestita con delega di FEM fornita a soggetti "Fiduciari" atti a verificare il contenuto dei messaggi e a inoltrare al Titolare del Trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. FEM ha identificato come fiduciari per tutta l'organizzazione i Responsabili interni del Trattamento (in relazione al settore di appartenenza) e gli Amministratori di Sistema.
6. La posta elettronica certificata di FEM può essere usata solo dagli incaricati individuati dalla Direzione Generale per scopi esclusivamente professionali legati ad attività lavorativa.

17 INTERNET

1. Richiamate le disposizioni di cui all'art. 5, comma 1 del Regolamento ICT ("Internet"), il servizio di accesso ad *Internet* (tramite *PC*, *tablet* o *smartphone* aziendali) è fornito solo per ragioni professionali connesse alla propria attività lavorativa all'interno o per conto di FEM. Essendo uno strumento di lavoro, gli utenti cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo.
2. Secondo le disposizioni previste dal Regolamento ICT all'art. 8 ("Controllo"), il numero, la durata ed il contenuto degli accessi ad *Internet* sono costantemente registrati. La consultazione di tali registrazioni avviene secondo le modalità descritte al punto 12 della presente Procedura.
3. Per prevenire eventuali abusi nell'uso di Internet o per ragioni di sicurezza connesse a visitazione di sorgenti pericolose per la diffusione e l'infezione (*malware*, spyware, *ramsonware*), il servizio di navigazione *internet* è stato comunque provvisto di filtri d'accesso.
4. Si devono comunque osservare le seguenti regole di navigazione della rete *Internet*:
   a) È tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende coperti da *copyright*, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di *software* che non sia specificatamente licenziato per essere utilizzato all'interno dell'azienda;
   b) È tassativamente vietato navigare siti e scaricare materiale pericolosi/vietati o aventi contenuti illegali (contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terrorismo o comunque inappropriato o illegale);
   c) È vietato effettuare copia non autorizzata di materiale coperto da *copyright*, compresa la digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
   d) È vietato il *download* e la condivisione di file in modalità *peer-to-peer*;
   e) È vietato immettere sulla rete o sui *server software* dannoso per i sistemi o comunque non autorizzato;
   f) È vietato utilizzare l'infrastruttura tecnologica aziendale per procurarsi e diffondere materiale in violazione con le normative vigenti;
   g) È vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;
   h) È vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'*host* dell'Utente (*sniffing*) a meno di specifiche attività e compiti dell'Utente, formalmente autorizzati dal proprio Responsabile.

18 ACCESSO DA REMOTO - VPN

Il collegamento alla rete aziendale da remoto attraverso VPN e *software* dedicato è autorizzato dal Responsabile del richiedente per esigenze di lavoro nelle modalità previste dalla FEM. Per motivi di sicurezza gli accessi realizzati dagli utenti da remoto attraverso VPN sono registrati.

19 GESTIONE DI DATI E INFORMAZIONI ATTRAVERSO SISTEMI *WEB CLOUD*

È vietato il salvataggio di dati e informazioni di carattere aziendale in sistemi *cloud* (ad esempio *Dropbox, iCloud, Evernote, ecc.*) in relazione ai quali FEM non abbia sottoscritto apposito contratto di utilizzo o comunque non preventivamente concordati ed autorizzati dalla Direzione Generale o dal Responsabile della RSIC. Più in generale, tutte le attività di *storage* di massa (in sistemi virtuali o dispositivi fisici) devono essere condotte nel rigido rispetto

delle previsioni in tema di tutela della riservatezza e protezione dei dati di cui al Regolamento ICT, fermo restando che – ai sensi del predetto Regolamento ICT - gli utenti che conservano dati, documenti e/o qualsivoglia informazione rilevanti per FEM su sistemi informatici non previamente censiti e approvati da FEM si assumono l'esclusiva responsabilità dei medesimi e di eventuali danni a FEM ovvero a terzi causati dalla loro perdita o sottrazione.

20 COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO *SOCIAL MEDIA*

È assolutamente vietato pubblicare in *internet* attraverso *Social media* personali, *forum*, *chat*, *blog*, siti *internet*, dati ed informazioni di carattere aziendale e di personale dipendente (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc.) non autorizzati dalla Direzione Generale.

21 UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE

Al termine dell'utilizzo dei supporti di memorizzazione contenenti dati (chiavette USB, *Hard Disk* interni ed esterni), questi dovranno essere cancellati, per eliminare ogni informazione contenuta prima di autorizzarne qualunque tipo di nuovo utilizzo. In caso di smaltimento dei supporti di memorizzazione, è fatto obbligo anche a carico dell'Utente assegnatario, la distruzione o danneggiamento fisico che ne renda impossibile il recupero del contenuto.

22 SERVIZI DI TELEFONIA

1. Su richiesta del rispettivo Dirigente, i dipendenti/collaboratori che ne abbiano necessità in funzione della mansione sono dotati di un telefono fisso o mobile. In alcuni casi l'apparato fisico potrà essere sostituito da un software (*SoftPhone*) associato al proprio numero interno.
2. L'assegnazione può essere permanente o temporanea e decade:
   a) Alla cessazione del rapporto di lavoro;
   b) Alla revoca del servizio da parte del Dirigente di riferimento;
   c) In caso di comprovato abuso da parte dell'assegnatario.
3. L'Utente si impegna a mantenere in efficienza e in buono stato il telefono concesso in uso, e a proteggere lo stesso da usi impropri o abusi commessi da terzi.
4. Nel caso di strumento mobile l'Utente si impegna a custodirlo con le dovute precauzioni per prevenirne il danneggiamento o furto. In caso di danneggiamento, la sua sostituzione avviene dietro refusione dei costi inerenti l'attività di riparazione, approvvigionamento e ripristino funzionale del nuovo, fissati in Euro 10,00.
5. In caso di furto l'Utente si impegna a darne immediata comunicazione a FEM e farne denuncia di furto presso le Autorità competenti secondo le procedure previste al momento dell'evento.
6. Richiamato l'art. 5, commi 1 e 7 del Regolamento ICT, in casi di emergenza è consentito l'uso della rete telefonica fissa e cellulare FEM per scopi personali.
7. È possibile l'utilizzo della telefonia mobile per scopi personali con tariffazione aziendale, previa attivazione della contabilità separata delle chiamate private (*dual-billing*) e con opportuno utilizzo atto a separare il traffico personale da quello aziendale.
8. L'Utente si impegna ad utilizzare il servizio dati telefonia mobile, conformemente alle disponibilità del *bundle* fornito, e ad interrompere ogni utilizzo nel caso di recepimento dell'avviso di supero soglia (SMS) da parte del *Provider*. L'utilizzo di applicazioni e servizi tramite smartphone (installazione "app", navigazione *internet*, utilizzo *e-mail* ecc) è soggetto alle stesse regole esposte nei punti 16, 17, 19 della presente Procedura.

23 POSTAZIONI DI LAVORO

1. L'Utente si impegna a mantenere in efficienza e in buon stato la postazione concessa in uso, e a proteggere la stessa da usi impropri o abusi commessi da terzi.
2. Le postazioni di lavoro sono fornite con un insieme di *software* di utilizzo comune precaricato a bordo. L'utente può chiedere alla RSIC, l'installazione di ulteriore *software* necessario all'attività lavorativa, se debitamente

licenziato per FEM e fornito delle chiavi di attivazione. In tale ipotesi l'Utente si assume la piena respondabilità circa le eventuali violazioni delle norme in tema di diritto d'autore e proprietà intellettuale.

3. È fatto carico agli utenti di controllare lo stato dei dispositivi *hardware/software* concessi in uso (tra cui il sistema *antivirus*), comunicando alla RSIC eventuali anomalie o malfunzionamenti.
4. Fatti salvi eventuali accordi con la RSIC, è vietato all'Utente:
   a) Effettuare qualsiasi modifica alla configurazione del sistema *hardware/software* concesso in uso;
   b) Effettuare qualsiasi variazione al sistema operativo;
   c) Utilizzare *software* installato o portatile non debitamente licenziato. Diversamente l'Utente si assume la piena responsabilità circa la violazione delle norme in tema di diritto d'autore e di altri diritti di proprietà intellettuale, esonerando FEM da ogni e qualsivoglia responsabilità in relazione all'abuso.
5. Per motivi di sicurezza è in particolare vietato l'utilizzo di collegamenti non sicuri (*wireless* esterni, *Internet Key*, ecc.) su postazioni collegate alla rete FEM.
6. L'acquisto ed il collegamento alla rete di *Personal Computer* non *standard* (ad esempio, Apple) è consentito a fronte di documentate esigenze applicative. Rimane inteso che su queste macchine non verrà fornita assistenza né *hardware* né *software* e non si garantisce il pieno funzionamento di tutti gli applicativi in uso presso FEM.
7. La riformattazione per l'installazione del sistema operativo Linux sui *Personal Computer* forniti da FEM è consentita esclusivamente previa richiesta con assenso da parte della RSIC. È fatto obbligo all'utenza di non rimuovere alcuna utenza root configurata, diversamente di concordare e configurare un'utenza con privilegi *root* per la dovuta gestione. È altresì fatto obbligo di richiedere alla RSIC gli opportuni parametri per la configurazione e messa in rete del dispositivo. Rimane inteso che su queste macchine non verrà fornita l'assistenza software ma solamente quella *hardware* e non si garantisce il pieno funzionamento di tutti gli applicativi in uso presso FEM.

24 RIPRESE VIDEO-AUDIO-FOTOGRAFICHE ALL'INTERNO DELLE AREE DEL TITOLARE

1. Personale interno: per ragioni connesse alla propria attività lavorativa devono essere autorizzate dal proprio Responsabile. Le immagini riprese devono essere utilizzate esclusivamente per finalità lavorative e non devono essere divulgate al di fuori del contesto lavorativo per cui sono state realizzate. Al di fuori di questa casistica al personale interno è vietato effettuare foto/videoriprese/audio, in qualunque area del Titolare, a meno che non sia stato preventivamente e formalmente autorizzato dalla Direzione Generale.
2. Terzi esterni: di norma, è vietato a terzi esterni di effettuare foto/videoriprese/audio, in qualunque area di FEM. Eventuali eccezioni devono essere autorizzate dalla Direzione Generale, valutando caso per caso. Il personale interno referente della visita del terzo esterno è tenuto a far rispettare queste prescrizioni, informando tempestivamente la Direzione Generale di eventuali inosservanze.
3. In ogni caso tutte le foto/videoriprese/audio devono essere realizzate rispettando i diritti delle singole persone eventualmente coinvolte nelle suddette riprese.

25 SERVIZI DI CALCOLO COMPUTAZIONALE *High Performance Computing*

L'uso dei *Sistemi High Performance Computing* è soggetto alle regole addizionali descritte nell'Appendice A.

Appendice A

Regole addizionali per l'uso dei Sistemi High Performance Computing

I – Utenti dei Sistemi *High Performance Computing* (da ora "HPC")

1. Tutte le Unità di ricerca possono utilizzare i sistemi HPC richiedendo l'accesso secondo la procedura di seguito descritta (punto II.2)
2. I responsabili di dipartimento individueranno delle figure che faranno parte di un tavolo chiamato "*Cluster-Strategic*". Questo tavolo prenderà decisioni strategiche a proposito dei Sistemi HPC.
3. I Responsabili dei dipartimenti che utilizzano i sistemi HPC eleggeranno uno o più Utenti di un secondo tavolo chiamato "*Cluster-Technical*" tra gli utilizzatori del *cluster*. Questo tavolo prenderà decisioni tecniche a proposito dei Sistemi HPC.
4. Tutte le altre richieste dovranno essere indirizzate al *Cluster-Strategic* (cluster-strategic@fbk.eu).

II – Utilizzo dei Sistemi HPC

1. Gli Utenti devono utilizzare *Secure Shell* (SSH) per collegarsi ai Sistemi HPC e *Secure Copy Protocol* (SCP) per trasferire file all'interno o all'esterno dei Sistemi HPC. I sistemi non accetteranno connessioni da altri protocolli. Dall'interno dei sistemi HPC, per motivi di sicurezza, non saranno consentite connessioni verso l'esterno.
2. L'accesso al Cluster potrà essere richiesto secondo la seguente procedura:
    1. Validazione richiesta Utente da parte di un membro *Cluster-Technical*
    2. Abilitazione accesso zona privata portale HPC (https://hpc.fmach.it)
    3. Invio form con chiave pubblica ssh da parte dell'Utente richiedente.
3. I *computer* che accettano connessioni SSH, chiamati "*Logon Server*", agiranno come dei *front-end*. Potranno essere usati per editing, compiling/debugging di piccole applicazioni e per la preparazione e la sottomissione di esecuzioni *batch*.
4. Non è consentita l'esecuzione di programmi che utilizzano pesantemente la CPU dei *logon server*. Gli applicativi di questo tipo (targz, *compile* e *debug sessions*, ecc.) devono essere eseguiti attraverso il sistema di *code*.
5. Il trasferimento dei dati da e verso i Sistemi HPC sarà possibile utilizzando SCP da *file server* esterni verso file server interni.
6. Tutti i *job* devono essere eseguiti attraverso il sistema di code. Saranno disponibili diversi tipi di *code* per diversi scopi.
7. Non sarà possibile connettersi direttamente ai nodi di calcolo dai *Logon Server*: sessioni interattive su nodi specifici potranno essere effettuate attraverso il sistema di *code*.
8. Il *debug* dovrà essere eseguito su una coda.
9. Ogni nodo ha un disco che potrà essere usato come scratch locale per memorizzare *file* temporanei durante l'esecuzione di *job*. Le dimensioni dello spazio variano da nodo a nodo. I dati memorizzati in questo spazio non saranno visibili dagli altri nodi o dai logon server. Gli Utenti sono incoraggiati a copiare i propri dati dai file server sullo *scratch* locale e a riportarli indietro alla fine del *job*. ~~Tutti~~ i dati più vecchi di una settimana, presenti nelle aree di *scratch*, saranno cancellati dopo un avvertimento.

III – Allocazione delle risorse dei Sistemi HPC

1. Normalmente i nodi sono utilizzati in modalità condivisa. Gli Utenti con la necessità di utilizzare nodi in modo esclusivo per un lungo periodo di tempo dovranno effettuare una richiesta al proprio rappresentante cluster technical perchè la possa sottoporre per relativa approvazione specificando sul calendario condiviso il tempo e il numero stimato. Ogni unità potrà prenotare in modo esclusivo una quantità limitata di nodi. Questi saranno riservati al più presto possibile a partire dalla data richiesta
2. Al momento della sottomissione dei job l'Utente dovrà specificare l'utilizzo massimo di RAM. Un GByte di RAM dovrà essere riservato per il sistema operativo. I *job* che eccedono i suddetti limiti saranno terminati senza ulteriore comunicazione.
3. È consigliato l'uso di *job checkpointed*.
4. Le quote di spazio disco sono gestite a seconda delle esigenze specifiche ricordando che si tratta di risorse condivise tra ~~tutti~~ i dipartimenti. È caldamente consigliato concordare con l'amministratore di sistema una politica di cancellazione/archiviazione dei dati obsoleti e di accesso non più urgente su media meno pregiati (es. tape libraries).
5. Le unità che hanno necessità di job con particolari caratteristiche potranno farne richiesta a Cluster Technical.

IV – Job monitoring

1. Il sistema avvertirà gli Utenti quando un loro *job* è:
    1. terminato (specificando il motivo);
    2. sospeso (specificando il motivo);
    3. ripreso;
    4. in esecuzione da lungo tempo.
2. Il sistema può essere configurato dagli Utenti per ricevere anche i seguenti avvertimenti:
    a. *Job* partito;
    b. *Job* finito.