FONDAZIONE
BRUNO KESSLER

Regolamento Privacy
della Fondazione Bruno Kessler

Regole di comportamento in materia di trattamento dei dati personali e aziendali, di utilizzo degli strumenti e dei sistemi informatici

Approvato con delibera del Consiglio di Amministrazione n. 15/17 del 20 dicembre 2017

Sostituisce ed integra la precedente Policy per l'utilizzo dei sistemi informatici nella sua ultima versione aggiornata al 17 maggio 2013

Modificato con delibera del Consiglio di Amministrazione n. 08/19 del 29 gennaio 2019

FONDAZIONE
BRUNO KESSLER

I. INTRODUZIONE

1. PREMESSA

Preservare la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni a tutela della dignità delle persone fisiche, delle libertà fondamentali e del valore del capitale intellettuale della Fondazione. Questo l'obiettivo del presente Regolamento che si inserisce nel contesto della generale disciplina in materia di Privacy e nel sistema normativo che regola l'organizzazione, i processi e le funzioni della Fondazione.

Le risorse informatiche e telematiche messe a disposizione da FBK costituiscono uno dei suoi punti di forza, ma nello stesso tempo, possono essere fonte di rischio per la sicurezza delle informazioni trattate e per l'immagine di FBK stessa. Per questo motivo il loro utilizzo deve sempre ispirarsi a criteri di liceità, correttezza e trasparenza.

L'individuazione di regole precise e chiare per l'utilizzo degli strumenti informatici e il trattamento dei dati personali e aziendali di FBK rappresenta un passaggio obbligato per assicurare una ottimale gestione delle funzioni della Fondazione.

Sono questi gli elementi che, nel contesto della disciplina in materia di privacy, hanno determinato FBK ad elaborare, adottare ed aggiornare il presente Regolamento, che sostituisce ed integra la precedente Policy per l'utilizzo dei sistemi informatici nella sua ultima versione aggiornata al 17 maggio 2013.

2. TUTELA DEL LAVORATORE

Il luogo di lavoro è una formazione sociale rispetto alla quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità di ciascuno in modo da garantire, in una cornice di reciproci diritti e doveri, l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.

3. SCOPO, CAMPO DI APPLICAZIONE E DESTINATARI

Lo scopo del presente Regolamento è quello di definire un insieme di norme comportamentali a cui tutti i dipendenti, i collaboratori, le eventuali terze parti e - in generale - i soggetti interni ed esterni che operano per FBK devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni.

Il presente Regolamento è realizzato in conformità a quanto previsto dal Regolamento Europeo n. 2016/679 – General Data Protection Regulation (da ora "GDPR"), dal Decreto Legislativo n. 196/2003 - Codice in materia di protezione dei dati personali – (da ora "Codice") così come novellato ed integrato dal Decreto Legislativo n. 101/2018 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679, e dai Provvedimenti del Garante.

Il presente Regolamento è destinato ai seguenti soggetti (da ora "soggetti"):

Soggetti interni:

- componenti degli Organi statutari
- dipendenti
- collaboratori coordinati e continuativi
- personale presente in FBK a fronte di accordi di distacco o di un comando
- dipendenti provinciali messi a disposizione di FBK
- consulenti e collaboratori occasionali
- affiliati (Alti profili, Affiliated fellows, Visiting fellows, PhD students, Scholars, High School fellows).

Soggetti esterni:

- imprese fornitrici di beni, servizi o lavori che operino con la Fondazione, indipendentemente dal rapporto giuridico sottostante, ed i loro dipendenti o collaboratori
- personale di altre entità presenti in FBK in forza di convenzioni o accordi inter-istituzionali
- visitatori e ospiti di vario genere.

II. DEFINIZIONI

1. Sono di seguito riportate le principali definizioni privacy.

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.

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

Dati particolari (ex 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.

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

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.

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.

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.

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.

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.

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.

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

Violazione di dati personali (Data Breach): 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. Di seguito sono riportate le definizioni relative alle figure privacy.

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

Titolare del trattamento: Fondazione 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.

Contitolare del trattamento: Titolare del trattamento che determina congiuntamente ad altro 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.

Responsabile esterno del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. Il Responsabile esterno 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.

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

Responsabile Interno del trattamento dei dati personali: soggetto interno alla Fondazione cui viene affidata la responsabilità per i trattamenti di dati personali riconducibili al relativo ambito di competenza. Tale soggetto coincide con un Responsabile di articolazione organizzativa.

Incaricato/autorizzato interno al trattamento: soggetto interno alla Fondazione autorizzato a compiere operazioni di trattamento di dati personali, sulla base dei regolamenti adottati e delle istruzioni impartite dal Titolare e/o dal Responsabile Interno del trattamento.

Amministratore di sistema: persona fisica o giuridica nominata dal Titolare e preposta alla gestione e sicurezza dei sistemi informativi attraverso l'applicazione delle misure necessarie al mantenimento della riservatezza, disponibilità e integrità del dato personale trattato.

Responsabile della gestione autonoma di strumenti informatici di proprietà di FBK: soggetto interno che gestisce in autonomia strumenti informatici di proprietà della Fondazione e che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato e dei dati di cui FBK è Titolare.

Responsabile della Protezione dei Dati (Data Protection Officer - DPO): persona fisica nominata dal Titolare 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, assiste il Titolare sulla valutazione di impatto privacy e sull'analisi del rischio e rappresenta il punto di contatto per interessati e Garante Privacy.

3. Di seguito sono riportate alcune altre definizioni utili alla corretta gestione dei processi di trattamento dei dati personali.

Badge: tesserino con chip elettronico di riconoscimento.

Pass: tesserino cartaceo senza identificativo.

Strumenti informatici: stampanti, laptop, computer da tavolo, telefoni fissi, smartphone, tablet, e-book reader, telecamere IP, e, in generale, qualsiasi dispositivo in grado di connettersi a una rete IP.

Data Center: locale ad accesso limitato che ospita i server, i sistemi di calcolo e i dispositivi di networking, oltre che i sistemi di storage su cui sono residenti i dati.

Cloud Pubblica: modello di conservazione dati su computer in rete dove i dati stessi sono memorizzati su molteplici server virtuali generalmente ospitati presso strutture di terze parti o su server dedicati.

III. MODELLO ORGANIZZATIVO

1. CLASSIFICAZIONE DELLE INFORMAZIONI

Il patrimonio informativo di FBK (costituito da tutti i dati e le informazioni trattati nei diversi processi, tra i quali anche i dati personali) può essere classificato secondo i seguenti criteri:

Dati e informazioni pubbliche: sono le informazioni liberamente trattabili da soggetti attraverso i mezzi di comunicazione messi a disposizione da FBK (sito internet, pubblicazioni, comunicati, ecc.). Queste informazioni non richiedono da parte del soggetto particolari attenzioni di riservatezza. La divulgazione di tali informazioni non presenta implicazioni per FBK in quanto si tratta di informazioni pubbliche che possono essere diffuse.

Dati e informazioni interne: sono le informazioni che possono essere trattate dai soggetti esclusivamente all'interno dei processi e del contesto organizzativo di FBK attraverso i canali istituzionali messi a disposizione da FBK (e-mail, intranet, aree di scambio su server e computer, ecc.). Queste informazioni richiedono da parte del soggetto una particolare attenzione nel trattamento, in quanto la loro divulgazione rappresenta una violazione dei vincoli di riservatezza ai quali è legato ogni soggetto con un possibile impatto legale (per esempio, violazione della privacy), a meno di essere rielaborate in modo da essere declassate a livello pubblico.

Dati e informazioni riservate: sono le informazioni che possono essere trattate da gruppi di soggetti autorizzati in virtù del ruolo e di una precisa finalità di trattamento individuata dal Titolare o dal Responsabile del trattamento. Tali informazioni devono essere comunicate solo a soggetti legittimati, valutando lo strumento di comunicazione più appropriato messo a disposizione da FBK in quanto la loro diffusione può avere un rilevante impatto legale (per esempio, violazione della privacy), d'immagine e di competitività per FBK.

Dati e informazioni strettamente riservate: sono le informazioni che possono essere trattate esclusivamente da determinati soggetti in base al ruolo ed alle responsabilità ricoperte in FBK. La divulgazione di tali informazioni può produrre gravi danni legali (per esempio, violazione della privacy), di immagine e di competitività per FBK.

2. MODELLO ORGANIZZATIVO DI RESPONSABILITÀ PRIVACY

In conformità con il GDPR, FBK ha definito e formalizzato un Modello Organizzativo di responsabilità privacy finalizzato al corretto trattamento dei dati personali. Tale modello è coerente con l'organigramma della Fondazione.

In occasione dell'aggiornamento annuale dell'organigramma generale, la Fondazione, in qualità di Titolare del trattamento dei dati personali, aggiorna anche la linea delle responsabilità interne in materia di trattamento dei

dati personali, individuando nei Responsabili delle articolazioni organizzative comunque denominate (ad esempio, Centri, Linee/Aree ad Alto Impatto, Unità, Servizi, …) i Responsabili Interni del Trattamento dei dati personali relativamente ai processi riconducibili alla loro esclusiva competenza. Tali soggetti sono nominati formalmente a valle di una formazione specifica.

Coloro che sono a capo di un progetto che implica il trattamento di dati personali, e non sono contemplati nel Modello Organizzativo di responsabilità privacy, sono tenuti ad adottare una policy *ad hoc* configurata sulle specifiche esigenze del caso (c.d. Privacy by Design). Essi adotteranno tale policy in coordinamento con il Titolare e per il tramite dell'Unità Prevenzione della Corruzione, Trasparenza e Privacy e con il coinvolgimento del Responsabile della Protezione dei Dati personali.

3. FBK QUALE RESPONSABILE ESTERNO DEL TRATTAMENTO

In ragione della stipula di contratti, convenzioni, accordi, progetti con soggetti esterni la Fondazione può essere nominata "Responsabile esterno del Trattamento dati ai sensi dell'art 28 del GDPR" quando le vengono affidati compiti specifici per i quali è previsto un trattamento di dati personali per finalità proprie di un soggetto affidatario (che risulta essere Titolare degli stessi).

In tutti questi casi, la Fondazione – anche in fase di stipula degli atti di cui sopra - individua il Responsabile Interno del Trattamento.

4. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Il Registro delle attività di trattamento è un documento di censimento e analisi dei trattamenti effettuati dal Titolare. Il Registro deve essere tempestivamente compilato e mantenuto costantemente aggiornato da ciascun Responsabile Interno del trattamento dei dati personali poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

IV. POLICY DI COMPORTAMENTO

1. PRINCIPI GENERALI DEL TRATTAMENTO

Trattare un dato personale rappresenta qualunque operazione o complesso di operazioni realizzate su un dato personale ed effettuate anche senza l'ausilio di strumenti elettronici. Il trattamento di un dato personale, per essere lecito, corretto e trasparente, deve sempre avvenire secondo alcuni principi generali privacy, che possono essere considerati vincoli inscindibili al trattamento dei dati personali. È importante chiedersi sempre se questi vincoli siano rispettati e solo ad una risposta sempre positiva possiamo avere la certezza che la privacy di una persona sia rispettata. In particolare quando avviene un trattamento di dati personali devono sempre essere rispettati i seguenti principi generali:

- Il rispetto della dignità dell'interessato, cioè della persona fisica di cui si stanno trattando i dati personali.
- Il rispetto dei principi di liceità, correttezza e trasparenza: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentali. Quanto alla trasparenza, tutte le informazioni destinate al pubblico o all'interessato devono essere concise, facilmente accessibili e di facile comprensione; il linguaggio utilizzato deve essere semplice e chiaro.

- Il rispetto del principio di limitazione della finalità: gli scopi del trattamento devono essere determinati, espliciti e legittimi, e successivamente trattati in un modo che non sia incompatibile con tali scopi (salvi gli ulteriori trattamenti per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica o storica, o per fini statistici).
- Il rispetto del principio di minimizzazione dei dati: i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Nello specifico, i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'uso di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o altre opportune modalità che permettano di identificare l'interessato solo in caso di necessità ('principio di necessità').
- Il rispetto del principio di esattezza: i dati trattati devono essere esatti e, se necessario, aggiornati, pertanto devono essere adottate tutte le misure ragionevoli per cancellare o rettificare i dati inesatti rispetto alle finalità per le quali sono trattati.
- Il rispetto del principio di limitazione della conservazione: i dati trattati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario al conseguimento degli scopi per cui sono raccolti e trattati (salvo specifici obblighi di legge, trattamenti di archiviazione nel pubblico interesse o per finalità di ricerca scientifica o storica, o per fini statistici).
- Il rispetto del principio di integrità e riservatezza: i dati devono essere trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti dalla perdita, dalla distruzione e dal danno accidentale.

2. TRATTAMENTO DI DATI PERSONALI A FINI STATISTICI E DI RICERCA

L'attività culturale e l'attività di ricerca sono importanti vie per ampliare i confini della conoscenza, favorire la crescita delle personalità dei singoli individui e consentire il progresso sociale.

Per assicurare tali finalità può essere consentito il trattamento di dati personali. E' in quest'ottica che la disciplina in materia di trattamento di dati personali contempla misure semplificate in ambito di ricerca storica, scientifica e statistica. Tali misure non esentano tuttavia il Titolare dall'adozione di accorgimenti idonei a prevenire possibili violazioni dei diritti degli interessati. Nell'informativa agli interessati, infatti, devono sempre essere chiaramente esplicitati e resi noti gli scopi perseguiti dall'indagine statistica o di ricerca.

I dati personali trattati per scopi statistici e di ricerca non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti finalizzati a scopi di altra natura. Tali dati vanno conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.

Le disposizioni relative al segreto statistico e alla riservatezza dei dati personali non si applicano ai dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

Al fine di promuovere e sostenere la ricerca e la collaborazione in campo culturale, scientifico e statistico la Fondazione – con esclusione dei dati di natura particolare e giudiziaria - può comunicare e diffondere dati relativi ad attività di studio e di ricerca.

Il personale di ricerca della Fondazione è tenuto ad uniformare la propria attività di ricerca e studio alle regole deontologiche promosse dal Garante della Privacy[1] e che sono allegate al Codice di Comportamento della Fondazione.

[1] https://www.garanteprivacy.it/codice

3. PUBBLICAZIONE DI ATTI E DOCUMENTI E DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

La Fondazione garantisce il diritto alla riservatezza dei dati particolari/giudiziari, contenuti negli atti pubblicati nella pagina dell'Amministrazione Trasparente e sul sito istituzionale, mediante la non diretta identificabilità dei soggetti, cui tali dati si riferiscono o tramite il loro oscuramento.

4. RAPPORTI TRA DIRITTO D'ACCESSO E PROTEZIONE DI DATI PERSONALI

I presupposti, le modalità, i limiti per l'esercizio del diritto d'accesso a documenti amministrativi contenenti dati personali e la relativa tutela giurisdizionale restano disciplinati dalla L. 241/1990 e s.m.i. e dalle altre disposizioni di legge in materia, nonché dalla normativa in materia di trasparenza che disciplina il diritto di accesso, anche per ciò che concerne i dati particolari e giudiziari e le operazioni di trattamento, eseguibili in adempimento di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Quando il trattamento concerne dati idonei a rilevare lo stato di salute o la vita sessuale, il trattamento è consentito, se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Per quanto riguarda i limiti all'acceso civico generalizzato derivanti dalla protezione dei dati personali, si rinvia alle linee guida ANAC n. 1309/2016.

5. GESTIONE DEI LOCALI E DELLE RISORSE FISICHE

Tutti i locali e tutte le risorse fisiche di FBK devono essere utilizzati e custoditi con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un adeguato livello di sicurezza delle informazioni, attenendosi al presente Regolamento per garantire la sicurezza fisica di aree ed *asset* di FBK.

6. ACCESSO AGLI UFFICI ED AREE PROTETTE

Sede e uffici. L'accesso agli uffici, alle aree protette, alle aree riservate ed agli archivi cartacei, è permesso ai soggetti autorizzati muniti di badge personale, in base a precise e motivate esigenze lavorative.

I dati relativi ai transiti tracciati dal badge personale potranno essere resi disponibili ai responsabili dei suddetti uffici, aree e archivi per finalità di sicurezza e tutela del patrimonio.

Ulteriori e specifici accessi ad uffici ed aree protette potranno essere concessi e abilitati da parte dell'Unità Sicurezza e Protezione solo a seguito di preventiva e motivata richiesta scritta da parte dei vari rispettivi Responsabili.

I visitatori e gli ospiti di vario genere potranno avere accesso alle suddette aree di FBK esclusivamente previa registrazione all'accettazione, esibendo il pass di riconoscimento ricevuto all'atto di registrazione e accompagnati da un soggetto interno.

Data Center. L'accesso ai locali Data Center di FBK è permesso esclusivamente a personale autorizzato mediante sistema biometrico o badge personale.

In via eccezionale e per breve tempo, nel Data Center è consentito l'accesso anche a visitatori e ospiti di vario genere, purché autorizzati e accompagnati da personale FBK autorizzato. I visitatori e gli ospiti di vario genere dovranno essere adeguatamente istruiti dal personale autorizzato in merito alle caratteristiche dell'ambiente, ai

rischi presenti, alle norme comportamentali previste e alle procedure da attuare per prevenire o gestire situazioni di emergenza e di rischio.

Per motivi di sicurezza e per conservare la temperatura costante di esercizio, tutti i varchi di accesso devono restare aperti solamente per il tempo strettamente necessario al passaggio di persone e materiali.

Per motivi di sicurezza è inoltre previsto lo scatto di un'immagine fotografica a chiunque acceda al Data Center di FBK e tale immagine è immediatamente inviata al personale autorizzato al presidio del Data Center.

Le suddette regole valgono anche per il sito di Disaster Recovery.

7. GESTIONE E CUSTODIA DEL BADGE

Il badge personale viene rilasciato dall'Unità Sicurezza e Prevenzione, previa conclusione dell'iter di immissione dati. I tempi tecnici di predisposizione del badge sono mediamente di 5 giorni lavorativi. Il badge è considerato un oggetto strettamente personale; dovrà quindi essere custodito adeguatamente e non potrà essere ceduto neppure temporaneamente.

In caso di uso non autorizzato, il badge verrà immediatamente ritirato dal personale di sorveglianza e potranno essere prese misure sanzionatorie.

In caso di smarrimento del badge, dovrà essere effettuata pronta comunicazione all'Unità Sicurezza e Prevenzione che provvederà alla sua disattivazione. In caso di sostituzione, il nuovo badge verrà rilasciato dall'Unità Sicurezza e Prevenzione a titolo oneroso.

Al termine del rapporto con FBK, il badge dovrà essere restituito all'Unità Sicurezza e Prevenzione.

8. RIPRESE VIDEO-AUDIO-FOTOGRAFICHE ALL'INTERNO DI FBK

Qualsiasi ripresa video-audio-fotografica deve essere realizzata rispettando i diritti delle singole persone coinvolte.

Soggetti interni: per ragioni connesse alla propria attività lavorativa le riprese video-audio-fotografiche devono essere autorizzate dal proprio Responsabile. Tali riprese possono essere utilizzate esclusivamente per finalità lavorative e non possono essere divulgate al di fuori del contesto istituzionale in cui sono state realizzate.

Al di fuori di questa casistica è vietato effettuare riprese video-audio-fotografiche in qualunque area di FBK, salvo preventiva e formale autorizzazione del proprio Responsabile d'intesa con l'Unità Digital Communication e Grandi Eventi.

I soggetti interni potranno essere fotografati e/o ripresi in occasione di eventi, seminari e momenti di formazione e per la documentazione di attività istituzionali con particolare riferimento alle attività di ricerca. In questi casi, le immagini e le riprese potranno essere utilizzate per scopi e comunicazioni istituzionali.

Per rafforzare la sicurezza interna in un contesto organizzativo in cui le sedi della Fondazione sono accessibili a terzi, l'immagine del profilo personale deve rispettare standard determinati e la sua pubblicazione è, per impostazione predefinita, obbligatoria sulle Reti interne della Fondazione.

Soggetti esterni: è vietato effettuare riprese video-audio-fotografiche in qualunque area di FBK. Eventuali eccezioni devono essere autorizzate dall'Unità Digital Communication e Grandi Eventi. Il soggetto interno referente dei soggetti esterni presenti in Fondazione è tenuto a far rispettare queste prescrizioni.

9. POSTAZIONI DI LAVORO

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.

Scrivania pulita. La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

10. MISURE FISICHE DI CUSTODIA DI DOCUMENTI E ATTI CARTACEI

I dati cartacei ed i supporti cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi in armadi o cassettiere del contesto organizzativo in cui si opera. Tutti gli archivi sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti necessari per lo svolgimento delle mansioni lavorative. 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 particolari (ex sensibili) dovranno essere custoditi in armadi chiusi a chiave.

L'eliminazione fisica di ogni documento cartaceo o supporto informatico contenente dati e informazioni aziendali e/o personali deve essere effettuata solo utilizzando gli appositi strumenti.

Si raccomanda di non lasciare documenti incustoditi presso i dispositivi di stampa.

11. GESTIONE DEI DATI PERSONALI E AZIENDALI

Ogni soggetto è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo.

I dati e le informazioni potranno essere comunicate a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

È vietata la comunicazione di dati e informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del *know-how* ed alla redditività della Fondazione o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

È assolutamente vietata la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

Si ricorda, inoltre, che la diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione del presente Regolamento, 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.

12. STRUMENTI INFORMATICI

L'utilizzo degli strumenti informatici in dotazione è di carattere professionale. In deroga a tale principio FBK autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio dello strumento affidato utilizzato a fini

"privati" (ad esempio dislocazione di file dati, foto o filmati), dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.

Tutti gli strumenti dovranno essere bloccati e protetti da password, se lasciati incustoditi.

Gli strumenti dovranno essere automaticamente spenti o messi in modalità a basso consumo se non usati per più di un'ora, a meno di motivate esigenze di ricerca.

FBK mette a disposizione dei soggetti diversi tipi di reti:

a. Interna, riservata ai dispositivi informatici di proprietà di FBK gestiti centralmente;

b. Esterna, riservata ai dispositivi informatici privati o a quelli di FBK non gestiti centralmente;

c. DMZ, riservata ai server gestiti centralmente che devono offrire servizi all'esterno.

Gli Amministratori di Sistema sono gli unici ad avere accesso ai sistemi informatici gestiti collegati alle reti interne e DMZ FBK con privilegi di Amministratore o "root", sia locale che di rete. Durante determinati periodi in cui un soggetto si allontana da FBK è possibile alzare i privilegi locali dello stesso sulla postazione di lavoro portatile in dotazione. Lo strumento sul quale vengono modificati i privilegi di accesso dovrà essere, senza eccezioni, inizializzato e reinstallato al rientro.

Sulle reti interne FBK e sui dispositivi gestiti centralmente, non è consentito modificare in alcun modo il sistema operativo o le applicazioni installate dagli Amministratori di Sistema che rispettano le misure idonee di sicurezza.

FBK, inoltre, ha siglato una Convenzione specifica 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.

13. POSSIBILITA' DI GESTIONE AUTONOMA DEGLI STRUMENTI INFORMATICI DI PROPRIETA' DI FBK

Per assicurare la massima flessibilità alla ricerca, il soggetto interno afferente al solo Comparto Ricerca, previa autorizzazione del suo diretto Responsabile e dell'Amministratore di Sistema, può ricevere la completa delega della gestione di strumenti informatici di proprietà di FBK per esclusive finalità di ricerca scientifica. Gli strumenti così configurati non potranno essere collegati alle reti interne e DMZ FBK, ma dovranno essere utilizzati sulle reti esterne.

Il soggetto interno, al momento della scelta di questa particolare modalità di utilizzo, accetta la conseguente designazione quale "Responsabile della gestione autonoma di strumenti informatici di proprietà di FBK"figura che deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato e dei dati di cui FBK è Titolare. Per tali soggetti responsabili è prevista una attività propedeutica e periodica di formazione con il fine ultimo di fornire concetti di base riguardanti le misure adeguate di sicurezza ed i generali obblighi previsti dalla normativa vigente in materia di protezione dei dati personali.

Quelle che seguono sono le regole di utilizzo dei suddetti strumenti informatici gestiti in autonomia:

- l'accesso ad Internet sarà possibile con le stesse regole della rete Eduroam.
- L'accesso alla rete interna FBK sarà possibile attraverso la SSL VPN e seguirà le stesse regole valide per gli strumenti personali.
- Gli strumenti informatici saranno visibili tra di loro senza limitazioni di porte e protocolli.
- Gli strumenti informatici non potranno offrire servizi verso Internet né diretti né indiretti.

- Gli strumenti informatici saranno accessibili dalla rete interna in modo diretto e dall'esterno, per motivi di manutenzione, solo attraverso la SSL VPN.
- Gli strumenti informatici non dovranno interferire con il normale funzionamento della rete.
- La gestione in autonomia implica capacità di gestione e debug degli strumenti informatici. L'installazione del sistema operativo sarà a cura del richiedente. Non è previsto il backup. Le licenze Windows saranno a carico di FBK, mentre le licenze Linux saranno a carico del richiedente.
- Il supporto del Servizio IT, Infrastrutture e Patrimonio sarà limitato alla sola parte hardware come previsto dalla garanzia. Nessun supporto sarà previsto per problemi software.
- Sul sito del Servizio IT, Infrastrutture e Patrimonio sono presenti le istruzioni per il collegamento dei sistemi alla rete e le modalità di debug per la connessione alle reti.
- Nel caso lo strumento informatico sia condiviso tra più soggetti, il Responsabile della gestione in autonomia sarà il Responsabile dell'Unità di Ricerca.

La stessa procedura dovrà essere seguita anche da qualsiasi soggetto interno che utilizza smartphone e tablet di proprietà della Fondazione.

14. CUSTODIA DEGLI STRUMENTI INFORMATICI

Gli strumenti informatici di proprietà di FBK devono essere custoditi dal soggetto con cura e diligenza prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento ed evitando di lasciarli incustoditi in ambienti pubblici.

In caso di furto o danneggiamento di beni, il soggetto dovrà informare immediatamente il Servizio IT, Infrastrutture e Patrimonio, presentare formale denuncia alle autorità di pubblica sicurezza e consegnarne copia al Servizio sopra menzionato per l'attivazione degli atti formali di scarico e di attivazione delle coperture assicurative.

15. GESTIONE DELLE CREDENZIALI DI ACCESSO E DELLE PASSWORD

Le credenziali di autenticazione per l'accesso alla rete e per altri servizi vengono assegnate dal Servizio IT, Infrastrutture e Patrimonio e consegnate al soggetto dall'Unità Sicurezza e Prevenzione. Esse consistono in un codice per l'identificazione del soggetto (username), associato ad una parola chiave (password) riservata che può essere modificata dal soggetto e dovrà venir custodita dallo stesso con la massima diligenza e non divulgata. Ogni soggetto è responsabile della sicurezza e di qualunque operazione effettuata utilizzando le proprie credenziali. È proibito accedere alla rete e ai programmi con credenziali diverse dalle proprie o in maniera anonima.

In caso di necessità di rinnovo delle credenziali alla scadenza del rapporto di lavoro, le relative richieste dovranno essere legate ad un rapporto di affiliazione.

Per mantenere un rapporto attivo con quanti abbiano contribuito con la loro visione al raggiungimento degli obiettivi strategici, la Fondazione ammette la possibilità, previo nulla osta della Segreteria Generale, che il personale che abbia ricoperto una posizione di responsabilità mantenga l'accesso ai servizi Google e Microsoft trasformando il dominio e-mail in @exstaff-fbk.eu.

16. GESTIONE E PROTEZIONE DEI DATI

L'accesso ai dati è consentito nei limiti della propria funzione organizzativa e della propria attività lavorativa.

I dischi di rete presenti sui server di FBK sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia inerente all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale autorizzato.

Si ricorda che i dischi o altre unità di memorizzazione locali non sono soggette a salvataggio da parte del personale autorizzato. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo soggetto.

Il personale autorizzato può in qualunque momento procedere alla rimozione di ogni file o applicazione che reputerà pericolosa per la sicurezza sia sugli strumenti informatici dei soggetti, sia sulle unità di rete: di tale intervento ne è informato il soggetto interessato e il suo diretto Responsabile.

Il backup dei principali server di rete viene effettuato dagli Amministratori di Sistema, che conservano i backup degli ultimi cinque anni. I soggetti che trattengono dati di FBK in aree per cui non è previsto backup sono responsabili del salvataggio degli stessi e di eventuali danni a FBK o a terzi anche di natura civilistica causati dalla loro perdita o sottrazione.

Fermi restando i vincoli esistenti a tutela della privacy per il proprio personale, i soggetti devono essere consapevoli che i dati da loro trattati sui sistemi informatici di FBK possono essere di proprietà di FBK o comunque sotto la responsabilità della stessa. Proprio per garantire la sicurezza e l'integrità delle informazioni presenti sui sistemi informatici di FBK, non è possibile garantire in maniera assoluta, in caso di controlli, la segretezza delle informazioni.

La memorizzazione temporanea di dati su strumenti informatici privati è consentita a patto che i suddetti strumenti siano protetti in modo da non consentire l'accesso di estranei non autorizzati.

È vietato il salvataggio di dati e informazioni di carattere professionale in sistemi o *storage* di ***cloud pubblica*** non autorizzati dagli Amministratori di Sistema.

Lo *storage cloud* da utilizzare in alternativa ai dischi di rete presenti sui server di FBK è Team Drive, parte della G-Suite di Google. Per questo servizio si applicano tutti i criteri validi per i dischi di rete sui server di FBK fatto salvo il backup dei dati per cui vale quanto previsto in G-Suite.

In considerazione del fatto che la Fondazione si relaziona con Pubbliche Amministrazioni, quando si sviluppano software, applicazioni e codici che trattano dati personali, è necessario rispettare ed adottare le indicazioni fornite dall'Agenzia per l'Italia Digitale (AGID) circa le misure di sicurezza ICT, seguendo metodologie di sviluppo che tengano conto dei problemi di privacy e sicurezza informatica.

17. GESTIONE DELLA POSTA ELETTRONICA

L'assegnazione di una casella di posta elettronica di FBK (da ora "e-mail FBK") è di carattere professionale. In deroga a tale principio FBK autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio della casella di posta utilizzato a fini "privati" dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.

La Fondazione, in conformità alla disciplina in materia di privacy, prevede che ad ogni messaggio in uscita sia automaticamente aggiunto un breve testo di avviso al ricevente della natura potenzialmente riservata del messaggio.

I soggetti titolari dell'e-mail FBK sono responsabili dell'utilizzo della stessa e devono mantenere un corretto comportamento nell'utilizzo della posta elettronica. In particolare, i soggetti devono seguire le seguenti disposizioni:

- non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale, salvo specifiche esigenze di ricerca;
- prestare la massima attenzione nell'invio di e-mail contenenti dati personali, che devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alla finalità per la quale sono inviati;
- prestare la massima attenzione nell'inoltro di e-mail riportanti contenuti e indirizzi e-mail di precedenti comunicazioni;
- prestare la massima attenzione ad e-mail sospette, avvisando l'Amministratore di Sistema in caso di dubbi sulla provenienza/contenuto delle stesse;
- creare una sezione denominata "Posta personale" all'interno della propria casella di posta, alla quale gli Amministratori di Sistema non potranno accedere se non per gravi motivi di sicurezza informatica.

Per motivi di sicurezza informatica ed in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'accesso alla casella di posta del soggetto potrà essere gestita dagli Amministratori di Sistema su richiesta del Responsabile Interno del Trattamento del soggetto al fine di verificare il contenuto dei messaggi e ad inoltrare al Titolare del Trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

La Posta Elettronica Certificata (PEC) può essere utilizzata dagli Incaricati/Autorizzati solamente per motivi professionali.

18. UTILIZZO DELLA NAVIGAZIONE INTERNET

L'accesso a Internet è fornito principalmente per scopo professionali, per accedere a informazioni e contenuti necessari allo svolgimento dell'attività lavorativa. Essendo uno strumento di lavoro, i soggetti cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo. Come per la posta elettronica, FBK ne autorizza un moderato e ragionevole utilizzo privato, limitato ed ispirato a criteri di buon senso senza ostacoli all'attività professionale.

Il numero e la durata degli accessi a Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge e dal mancato rispetto del presente Regolamento. Gli eventuali controlli compiuti dagli Amministratori di Sistema potranno avvenire mediante un sistema di analisi dei file giornale. I soggetti devono seguire 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 di FBK;

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), salvo specifiche esigenze di ricerca;

c. è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso ma non limitato a digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;

d. è vietato utilizzare l'infrastruttura tecnologica di FBK per procurarsi e diffondere materiale in violazione con le normative vigenti;

e. è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;

f. è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host del soggetto (sniffing) a meno che questa attività non faccia parte dei compiti del soggetto e quindi formalmente autorizzata dagli amministratori di sistema;

g. è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.

19. ACCESSO INTERNET PER SOGGETTI ESTERNI

È previsto un sistema per consentire l'accesso e la navigazione in Internet a soggetti esterni.

Il numero e la durata degli accessi ad Internet sono costantemente registrati.

20. ACCESSO DA REMOTO - VIRTUAL PRIVATE NETWORK (VPN)

L'accesso dall'esterno alla rete di FBK è consentito esclusivamente attraverso precise modalità di connessione sicura, indicate sul sito del Servizio IT, Infrastrutture e Patrimonio . Ogni altro accesso è espressamente vietato.

21. USO DEI SISTEMI HIGH PERFORMANCE COMPUTING (HPC)

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

22. 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 professionale (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc..) che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how ed alla redditività di FBK o che possano violare i vincoli contrattuali e di legge connessi al rapporto con la Fondazione.

È assolutamente vietato divulgare notizie false.

È autorizzata la divulgazione di informazioni già rese pubbliche da FBK; in caso di dubbi in proposito, la struttura di riferimento è l'Unità Digital Communication e Grandi Eventi.

23. SISTEMI DI MONITORAGGIO RETE DELLA FONDAZIONE

Per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.) o per finalità di

controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, per il tramite degli Amministratori di Sistema e nel rispetto della normativa sulla privacy, accedere direttamente a tutti gli strumenti informatici di FBK.

Periodicamente e in presenza di anomalie, gli Amministratori di Sistema effettueranno verifiche di funzionalità approfondite che potranno determinare segnalazioni ed avvisi generalizzati diretti ai soggetti della funzione organizzativa in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

Gli Amministratori di Sistema effettuano inoltre forme di controllo di carattere impersonale sulla rete e su tutti i dispositivi che la compongono. I dettagli relativi ai controlli effettuati sono disponibili nell'Appendice B.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

FBK è tenuta comunque a denunciare all'autorità giudiziaria tutti i comportamenti contrari alla legge, anche rilevati da analisi di tipo impersonale.

24. UTILIZZO DELLA FIRMA DIGITALE

La Firma Digitale deve essere utilizzata esclusivamente dal proprietario della firma.

25. SISTEMA DI VIDEOSORVEGLIANZA

Il sistema di videosorveglianza è realizzato in alcune aree specifiche (adeguatamente indicate da cartelli informativi) con finalità di sicurezza e controllo per tutelare il patrimonio di FBK contro atti vandalici, accessi non autorizzati o guasti tecnici e strutturali, comportamenti illeciti e/o fraudolenti e per agevolare gli operatori nel controllo della sicurezza delle strutture.

L'accesso alle immagini videoregistrate è permesso esclusivamente per le finalità sopra indicate agli incaricati/autorizzati al trattamento ed in caso di necessità agli organi preposti delle forze dell'ordine.

Il Documento sulla Videosorveglianza viene adottato dal Responsabile della Videosorveglianza nominato dal Consiglio di Amministrazione ed aggiornato in base alle necessità.

26. SPECIFICI DIVIETI

Di seguito sono riportati specifici divieti:

a. alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
b. accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
c. accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
d. detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico o di soggetti concorrenti, pubblici o privati al fine di acquisire informazioni riservate;
e. svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati

o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

f. svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;

g. svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

h. svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

i. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;

j. caricare programmi non provenienti da una fonte certa e autorizzata dalla Società;

k. acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all'originalità/autenticità del software;

l. detenere supporti di memorizzazione di programmi non originali (DVD\CD\floppy);

m. installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di *underlicensing*;

n. utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;

o. utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;

p. distribuire software di proprietà della Fondazione a soggetti terzi;

q. realizzare codice software che violi copyright di terzi;

r. accedere illegalmente e duplicare banche dati.

27. PERDITA DELLE CONDIZIONI DI INCARICATO/AUTORIZZATO

In caso di perdita delle condizioni di Incaricato/Autorizzato al Trattamento o di cessazione del rapporto con FBK, valgono le seguenti regole operative:

a. Le credenziali per l'accesso ai sistemi e alla posta elettronica vengono disattivate.

b. È facoltà di FBK effettuare eventuali operazioni di conservazione di e-mail di carattere professionale di soggetti non più appartenenti all'organizzazione. Le e-mail nella "Posta personale" saranno, al contrario, cancellate.

Tali attività sono effettuate dagli Amministratori di Sistema autorizzati alla gestione della posta elettronica, che potranno pertanto avere accesso, per esclusive ragioni di carattere tecnico e solo ove non sia evitabile, a dati personali conservati all'interno delle caselle di posta.

Con il dovuto anticipo, il soggetto interno è tenuto ad attivare il risponditore automatico per notificare ad eventuali fornitori, partner, clienti od altri soggetti interessati, l'interruzione del proprio rapporto con FBK e - se del caso - per proporre un contatto interno alternativo.

Per quanto riguarda la restituzione degli strumenti informatici di proprietà di FBK, valgono le seguenti regole operative:

a. Smartphone e tablet devono essere restituiti al Servizio IT, Infrastrutture e Patrimonio.

b. Gli altri strumenti informatici affidati a soggetti del Comparto Ricerca devono essere restituiti al Responsabile dell'Unità di Ricerca di appartenenza.

c. Gli strumenti informatici affidati a soggetti del Comparto Amministrazione andranno restituiti al Servizio IT, Infrastrutture e Patrimonio.

28. VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

Per "violazione di dati" si intende la 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.

I casi di violazione di dati personali devono immediatamente essere segnalati al Responsabile della Protezione dei Dati personali (privacy@fbk.eu) assicurando così l'attivazione della procedura di gestione delle violazioni di sicurezza.

29. PRESCRIZIONE RESIDUALE

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, ciascun soggetto può rivolgersi al proprio Responsabile e all'Unità Prevenzione della Corruzione, Trasparenza e Privacy per ricevere le opportune istruzioni.

30. RESPONSABILITÀ E SANZIONI

È fatto obbligo a tutti i soggetti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione del presente Regolamento sono perseguibili con provvedimenti disciplinari e risarcitori previsti dal vigente Codice Disciplinare di FBK, nonché con tutte le azioni civili e penali consentite.

Chiunque non rispetti il presente Regolamento potrà essere soggetto all'immediata sospensione dell'accesso agli strumenti informatici.

31. AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto a revisione periodica, che potrà avvenire a seguito di cambiamenti organizzativi e normativi o necessità istituzionali. Tutte le future modifiche al presente Regolamento verranno opportunamente comunicate e rese pubbliche sul sito internet di FBK.

Letto ed approvato il 29 gennaio 2019

- prof. Francesco Profumo -

Presidente della Fondazione Bruno Kessler

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 operative di ricerca possono utilizzare i sistemi HPC richiedendo l'accesso o il supporto a help-it@fbk.eu.
2. I Responsabili delle Unità operative che utilizzano i sistemi HPC faranno parte di un tavolo chiamato "Cluster-Strategic". Questo tavolo prenderà decisioni strategiche a proposito dei Sistemi HPC.
3. I Responsabili delle Unità operative che utilizzano i sistemi HPC eleggeranno uno o più Utenti di un secondo tavolo chiamato "Cluster-Technical". 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. 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.
3. 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.
4. Il trasferimento dei dati da e verso i Sistemi HPC sarà possibile utilizzando SCP da file server esterni verso file server interni.
5. Tutti i job devono essere eseguiti attraverso il sistema di code. Saranno disponibili diversi tipi di code per diversi scopi.
6. 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.
7. Il debug dovrà essere eseguito su una coda.
8. 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 prenotazione 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. Tutti i *job* che eccedono i suddetti limiti saranno terminati.
3. È consigliato l'uso di *job checkpointed*.
4. Le quote di spazio disco sui file server sono gestite a livello di Unità. Ogni Unità potrà avere riservate diverse quantità di spazio.
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:
   a. terminato (specificando il motivo);
   b. sospeso (specificando il motivo);
   c. ripreso;
   d. 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.

Appendice B

Dettagli relativi alle attività di controllo svolte dagli Amministratori di Sistema

FBK gestisce i sistemi informatici e le reti anche attraverso strumenti che possono memorizzare temporaneamente dati relativi alla navigazione internet e al traffico telematico. In particolare si elencano:

1. Posta Elettronica - dati conservati:
   a. log del traffico SMTP generato dai server di posta elettronica;
   b. log dei messaggi non correttamente inoltrati (ritardi e/o mancate consegne);
   c. log dei messaggi intercettati dal sistema antivirus.
2. Traffico IP – corretto funzionamento del sistema, monitoraggio SLA, controlli di sicurezza:
   a. Log del traffico IP generato dai dispositivi informatici. Tale log comprende anche dati puntuali di navigazione riferibili all'indirizzo IP interno di provenienza della richiesta. I dati sono conservati per circa 26 settimane in un sistema accessibile solo dagli amministratori di sistema autorizzati, e non utilizzato normalmente per altre attività di FBK. 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.
3. Telefonia – corretto funzionamento del sistema:
   a. Log delle chiamate (numero chiamante, numero chiamato, durata).
4. Accesso alle reti - corretto funzionamento del sistema, monitoraggio SLA e controlli di sicurezza:
   a. Log di accesso alle reti dall'esterno e dall'interno.

Come indicato nelle Linee Guida del Garante per posta elettronica e internet, FBK non procederà in nessun caso a controlli non consentiti, quali:

- lettura e registrazione puntuale di messaggi di posta;
- riproduzione e memorizzazione delle pagine internet visitate;
- cattura dei caratteri digitati attraverso tastiera (fisica o virtuale);
- analisi occulta dei pc affidati in uso.