Procedura

Disciplinare Tecnico sull'utilizzo delle risorse di calcolo e rete

Parent process: PRDA – Proteggere i dati

The original updated file is available on the corporate document management system.

Emissione del documento

Questo documento ha seguito il seguente iter di ufficializzazione:

Iter di approvazione

Rev06	Aggiornamenti e modifiche normative, per il lavoro agile, per l'utilizzo dei dispositivi personali e migliorare la sicurezza.	Redazione	22/01/2022	PUGLIESE Roberto
		Validazione	07/02/2022	PASSUELLO Roberto
		Verifica	08/02/2022	COCOLO Euro
		Verifica	08/02/2022	FORGIARINI Laura
		Verifica	16/02/2022	RUSSO Livio
		Approvazione	23/02/2022	SVANDRLIK Michele
		Approvazione	24/02/2022	FRANCIOSI Alfonso

Registro delle revisioni precedenti

Rev05	Aggiornamento per gestione Database Software Aziendali.	Redazione	03/02/2017	PUGLIESE Roberto
		Redazione	03/02/2017	PUGLIESE Roberto
		Verifica	08/02/2017	Gruppo di Lavoro Documenti
		Verifica	08/02/2017	Gruppo di Lavoro Documenti
		Approvazione	03/02/2017	ZAMBELLI Mauro
		Approvazione	03/02/2017	ZAMBELLI Mauro

Indice

0 Scopo e campo di applicazione

I sistemi informatici, intesi come calcolatori (hardware), programmi applicativi (software) e reti di trasmissione dati, rivestono oggi un ruolo basilare nello svolgimento di ogni attività lavorativa.
L'estrema diffusione di tali risorse all'interno di Elettra - Sincrotrone Trieste S.C.p.A. (di seguito indicata come "Elettra" o la "Società"), pone l'accento sulla necessità di provvedere al mantenimento di un adeguato livello di efficienza e sicurezza.

Una precisa regolamentazione relativa all'utilizzo degli strumenti informatici in dotazione al "personale" è una misura di sicurezza indispensabile per:

- favorire il massimo livello di supporto alle attività della Società;
- garantire il rispetto delle leggi in materia di protezione dei dati personali e che prevedono l'adozione di idonee misure di sicurezza;
- evitare l'esposizione della Società a rischi sia patrimoniali che penali derivanti dall'inosservanza delle norme vigenti da parte del personale.

Posto che l'utilizzo delle risorse informatiche deve in ogni caso ispirarsi al principio della diligenza e della correttezza, Elettra ha adottato la presente Procedura, con il fine di illustrare al personale:

- le modalità operative per il corretto impiego degli strumenti messi a disposizione;
- le corrette procedure organizzative da seguire nell'utilizzo di tali strumenti;
- le misure di sicurezza più appropriate per assicurare la disponibilità e l'integrità dei sistemi informativi, della rete e dei dati trattati;
- i casi e le modalità in cui possono essere effettuati controlli da parte del datore di lavoro.

Con questo documento Elettra intende prevenire comportamenti, anche inconsapevoli, che possano dare origine a rischi o minacce per la sicurezza dei dati ed evitare l'esposizione a rischi derivanti dall'inosservanza delle norme vigenti.

1 Responsabilità

Le attività di configurazione, amministrazione e manutenzione delle risorse di calcolo e rete di proprietà Elettra in funzione presso il Laboratorio sono demandate al personale operante presso il Gruppo Informatica, ovvero, qualora segnalato, ad entità esterne dotate di specifiche competenze in materia. L'elenco degli amministratori di sistema/rete e dei Responsabili del trattamento dei dati interni ed esterni è disponibile nella sezione "Organigramma Privacy di Elettra - Sincrotrone Trieste S.C.p.A." della pagina https://www.elettra.eu/public/privacy/privacy.html.

2 Riferimenti

2.1 Riferimenti esterni

Il presente Disciplinare Tecnico viene adottato in conformità ed ottemperanza a:

Legge 300/1970 *"Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"*;

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito "GDPR";

Decreto Legislativo 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", novellato dal Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679"

Deliberazione del Garante per la protezione dei dati personali, dd. 1° marzo 2007, *"Linee Guida sull'utilizzo di posta elettronica e internet nei luoghi di lavoro"*; Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" e successive modifiche (*cfr. provvedimento del Garante dd. 25 giugno 2009*).

Decreto Legislativo 8 giugno 2001, n. 231 (in Gazz. Uff., 19 giugno, n. 140). – "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*"

Acceptable Use Policy AUP della rete GARR reperibile al seguente indirizzo:

https://www.garr.it/it/regole-di-utilizzo-della-rete-aup

Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale.

2.2 Definizioni

Le seguenti definizioni sono state riprese dal Glossario generale dei termini, delle definizioni e delle abbreviazioni, al quale si rimanda per la versione completa e aggiornata di tutte le definizioni di uso comune in Elettra.

DOCS-SCH-01

2.2.1 Risorse di calcolo e rete

Per “risorse di calcolo e rete” si intendono, ad esempio:
i server adibiti al calcolo (sistemi di calcolo centrali) amministrati dal Gruppo Informatica;
i server adibiti alla gestione di servizi essenziali (DNS, mail, Web, etc.), amministrati dal Gruppo Informatica;
i sistemi di “mass storage” amministrati dal Gruppo Informatica (Sistemi di Storage per i Dati Scientifici, Cloud, NAS etc.);
i sistemi dedicati ad attività, gruppi o esperimenti, adibiti a servizi specifici ed amministrati dal Gruppo Informatica;
i computer e le stampanti di pubblico utilizzo;
i personal computer, gli smartphone, i tablet;
gli apparati e servizi di rete cablata e/o wireless;
gli applicativi software acquistati e/o distribuiti da Elettra;
i servizi informatici o di rete, forniti in modo centralizzato da Elettra.

2.2.2 Accesso ad internet

L'accesso ad internet dalla rete locale di Elettra avviene attraverso la Rete Italiana dell'Università e della Ricerca Scientifica, denominata comunemente “Rete GARR”. L'uso di detta rete, da parte di Elettra e del suo personale (soggetti autorizzati all'accesso), è subordinato al rispetto delle regole descritte nel documento: Acceptable Use Policy AUP della rete GARR, disponibile alla pagina https://www.garr.it/it/regole-di-utilizzo-della-rete-aup .
Il documento Acceptable Use Policy AUP del GARR stabilisce che i soggetti autorizzati all'accesso alla rete GARR possono utilizzare la rete per tutte le proprie attività istituzionali.
Non è consentito, ad esempio:
fornire a soggetti non autorizzati all'accesso, il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing (connessione alla rete Elettra di macchine di terze parti), di hosting (inserimento nei server Web di pagine di terze parti) e simili;
utilizzare servizi o risorse di rete in grado di danneggiare, molestare o perturbare le attività di altre persone;
creare o trasmettere qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;
trasmettere materiale commerciale e/o pubblicitario non richiesto (“*spamming*”), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività.
La responsabilità del contenuto dei materiali prodotti e diffusi attraverso la rete è delle persone che li producono

	e diffondono. È pertanto rimesso alla correttezza dell'utente il buon utilizzo dell'accesso risultando il medesimo personalmente responsabile nel caso in cui adotti un comportamento scorretto.
2.2.3 Amministratori di sistema (e/o di rete)	Figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerati amministratori di sistema anche le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi [*Provvedimento del Garante dd. 27/11/2008 e successive modifiche dd. 25/06/2009*]. L'elenco completo degli Amministratori di sistema e/o di rete è disponibile e consultabile nella sezione "Organigramma Privacy di Elettra - Sincrotrone Trieste S.C.p.A." della pagina: https://www.elettra.eu/public/privacy/privacy.html.
2.2.4 Credenziali di autenticazione	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (es. username e password). [*Art. 4, comma 3) lett. d) del "Codice"*].
2.2.5 Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale [*Art. 4, paragrafo 1) del GDPR*]
2.2.6 Categorie particolari di dati personali (Dati sensibili)	Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2.2.7 Incaricati del trattamento dei dati personali	Persone istruite ed autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile del trattamento [*Art. 4, par. 10) ed Art. 29 del GDPR*]; Persone fisiche, espressamente designate mediante atto di nomina individuale, che operano sotto la responsabilità del titolare o del responsabile del trattamento, con specifici compiti e funzioni connessi al trattamento di dati personali [*Art. 2-quaterdecies del D.Lgs. n. 101/2018*]

2.2.8 Trattamento dei dati personali	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o 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 [*Art. 4, par. 2) del GDPR*]
2.2.9 Titolare del trattamento dei dati personali	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali [*Art. 4, par. 7) del GDPR*] Titolare del trattamento di Elettra - Sincrotrone Trieste è: Elettra - Sincrotrone Trieste S.C.p.A. di interesse nazionale - Strada Statale 14, km 163,5 in AREA Science Park - 34149 Basovizza -Trieste.
2.2.10 Responsabile della protezione dei dati	Persona fisica o giuridica designata dal titolare o dal responsabile del trattamento alla quale sono affidati i seguenti compiti: informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento; sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento [*Art. 39, par. 1) del GDPR*]
2.2.11 Utente	Per "utente" si intende il personale che per fini lavorativi utilizza una o più risorse di calcolo e/o di rete, messe a disposizione da Elettra, senza possedere accessi privilegiati alle risorse stesse.
2.2.12 Personale	Per "personale" si intendono dipendenti, collaboratori, partner, utenti delle linee di luce, associati, ospiti, dottorandi, borsisti, laureandi, specializzandi e stagisti.

3 Modalità operative

Il personale che utilizza le risorse di calcolo e di rete di proprietà di Elettra è tenuto a prendere conoscenza e ad attenersi a quanto riportato nel presente documento, ciò anche al fine di non compromettere la sicurezza degli strumenti elettronici di calcolo

presenti, escludere il rischio di commissione dei reati previsti dal D.lgs. 231/2001, nonché di salvaguardare l'immagine aziendale.

3.1 Responsabilità, diritti e doveri

3.1.1 Datore di lavoro / Titolare del trattamento

Secondo quanto prescritto dall'Art. 32 del GDPR, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti delle persone fisiche, il "Titolare del trattamento" e il "Responsabile del trattamento" mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

Il datore di lavoro, in conformità alle disposizioni di legge che garantiscono la tutela dei diritti e delle libertà fondamentali dei lavoratori, nonché del diritto alla riservatezza, si riserva di effettuare attività di controllo a campione o in seguito ad episodi che si configurano come incidenti di sicurezza:

- al fine di verificare la funzionalità e la sicurezza ed il corretto impiego dei sistemi;
- in conseguenza alla rilevazione di anomalie nel regolare funzionamento delle risorse informatiche (PC, server, apparecchiature di rete, software, ...);
- in caso di minacce gravanti sulla sicurezza dei sistemi;
- per il perseguimento di esigenze difensive (indebito utilizzo degli strumenti informatici societari);
- per provvedere alle necessarie attività di aggiornamento.

I controlli sono effettuati da personale qualificato (Amministratori di sistema o di rete), autorizzato dal datore di lavoro.

In particolare, al fine di tutelare la sicurezza e il buon funzionamento dei PC, degli smartphone, dei tablet e della rete e dei sistemi, la posta elettronica è sottoposta a controlli antivirus automatici al fine di prevenire la consegna al destinatario di messaggi risultati positivi ai test antivirus ovvero identificati come "spam", "phishing" o potenziali minacce.

Elettra può avvalersi di sistemi di controllo con la sola finalità di garantire la sicurezza nel trattamento dei dati e nell'uso della dotazione informatica. Le verifiche operate non mirano ad un controllo a distanza nei confronti dei lavoratori e sono attuate evitando interferenze ingiustificate sui diritti e sulle libertà fondamentali dei lavoratori.

Le attività relative all'uso del servizio di accesso ad Internet sono automaticamente registrate in forma elettronica (*log* di sistema), nel rispetto delle disposizioni di legge in materia e automaticamente cancellate in base alla normativa vigente.
I dati personali contenuti nei log possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste della Polizia delle Comunicazioni e/o dell'autorità giudiziaria;
- per l'erogazione del servizio;
- per l'analisi di malfunzionamenti;
- per l'effettuazione di statistiche sull'utilizzo delle risorse previa anonimizzazione dei dati.

Il datore di lavoro ha il diritto, anche avvalendosi delle figure preposte (Amministratori di sistema e/o di rete), di:

- accedere alle risorse di calcolo e rete ed ai locali che le contengono;
- di revocare, anche senza preavviso, l'accesso alle risorse di calcolo e rete, qualora esse siano utilizzate impropriamente o in violazione delle leggi vigenti.

Le attività sopra descritte dovranno essere sempre ispirate ai principi di correttezza e trasparenza, come previsto anche dallo Statuto dei lavoratori in materia di "uso di attrezzature munite di videoterminali".

In ogni caso, le informazioni e i dati raccolti ai sensi del presente documento possono essere utilizzati per tutti i fini connessi al rapporto di lavoro, nel rispetto di quanto disposto dal GDPR.

3.1.2 Amministratori di sistema (e/o di rete)

Gli amministratori di sistema e/o di rete, nell'ambito della loro attività, devono sempre operare nel rispetto di quanto descritto nel presente disciplinare tecnico, seguendo le politiche in materia di sicurezza adottate da Elettra e, più in generale, secondo quanto disposto dalle normative di legge vigenti.

Qualora venissero rilevate condizioni che pongano a rischio immediato la corretta funzionalità delle risorse di calcolo e rete e l'onere delle normali procedure limitassero l'efficacia e la tempestività degli interventi, gli Amministratori di sistema sarebbero autorizzati ad operare in autonomia per porre le apparecchiature interessate in condizioni di sicurezza.

3.1.3 Utenti

Le risorse di calcolo e rete di proprietà di Elettra, destinate alla ricerca scientifica, tecnologica ed alla gestione amministrativa e contabile societaria, possono essere utilizzate esclusivamente per le attività istituzionali, secondo le modalità descritte nel presente documento e, più in generale, secondo quanto disposto dall'Art. 32 del GDPR e dalle *"Acceptable Use Policy"* (AUP) della rete GARR.

Gli utilizzatori dei sistemi informatici e di rete sono tenuti a mantenere un comportamento corretto e ad evitare ogni indebito utilizzo delle risorse loro affidate, dei servizi e dei dati a cui possono accedere.

Ad esclusione di accessi temporanei di ospiti, visitatori, utenti, ecc. attraverso la rete "ST-GuestNet" previa assegnazione di una "*username*" e "*password*" fornita dalle segreterie di Elettra, l'accesso alle risorse di calcolo e rete è riservato al personale ed ai collaboratori di Elettra.

È consentito il collegamento alla rete locale di Elettra di computer non appartenenti a Elettra solo mediante specifica e preventiva autorizzazione da parte del Coordinatore del Gruppo di appartenenza (o dell'Amministratore Delegato di Elettra) che verificherà la necessità dell'utilizzo dello stesso per svolgere l'attività lavorativa. Su detti computer è in ogni caso vietata l'installazione di software con licenza d'uso registrata a nome di Elettra, a meno di specifici casi che lo permettano e che verranno verificati e autorizzati dall'Attività Sistemi e Servizi ICT.

Nel caso di dispositivi privati di altro tipo (cellulari, smartphone, tablet, …) da utilizzare per svolgere l'attività lavorativa, è necessaria l'autorizzazione dell'Amministratore Delegato di Elettra che dovrà essere richiesta dal Coordinatore del Gruppo di appartenenza.

L'accesso alle risorse di calcolo e rete, subordinato all'osservanza di quanto contenuto nel capitolo *"Misure minime di sicurezza"*, è autorizzato dal datore di lavoro a titolo personale e non può essere condiviso o ceduto, salvo i casi specificamente individuati di sistemi in uso, per ragioni funzionali, a più persone.

Gli utenti sono in ogni caso tenuti a segnalare prontamente al Responsabile della protezione dei dati ovvero all'Amministratore di sistema e/o di rete ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.

Il personale specificamente incaricato del trattamento dei dati personali provvederà a rendere disponibili le credenziali di autenticazione per l'accesso ai dati personali oggetto del trattamento medesimo, in modo da rendere possibile l'accesso in caso di prolungata assenza o impedimento che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

3.2 Misure minime di sicurezza

Elettra, in qualità di titolare del trattamento deve, secondo quanto disposto dall'Art. 32 del GDPR, provvedere ad adottare opportune misure di sicurezza a protezione dei dati e dei relativi sistemi con i quali viene effettuato il trattamento.
Gli utenti sono tenuti ad osservare le seguenti misure minime di sicurezza per la protezione dei dati personali e non:

- proteggere i propri account mediante password da adottarsi secondo le regole indicate al punto "*Regole per la scelta della password*";
- utilizzare programmi antivirus locali e verificare regolarmente che avvenga l'aggiornamento automatico delle cosiddette "definizioni di virus". L'Attività Sistemi e Servizi ICT è tenuta a fornire licenze e supporto per questa tipologia di operazioni;
- informarsi regolarmente ed adottare le "patch di sicurezza" o gli aggiornamenti relativi al sistema operativo utilizzato. L' Attività Sistemi e Servizi ICT si impegna a fornire il massimo supporto informativo e pratico;
- utilizzare un salvaschermo con password, attivabile automaticamente dopo un tempo prefissato non superiore ai 10 minuti, in caso di abbandono del proprio computer con una sessione attiva;
- monitorare costantemente il sistema. Ogni sospetto di possibile intrusione e ogni altro problema di sicurezza va immediatamente segnalato all'Amministratore di sistema e/o di rete, ovvero all'Attività Sistemi e Servizi ICT;
- mantenere preferibilmente i file su sistemi di immagazzinamento dati condivisi, remoti che sono sottoposti ad adeguate politiche di backup (Elettra Drive, online4, gitlab, ...);
- nel caso non sia possibile, per motivate ragioni, mantenere alcuni file su sistemi di immagazzinamento dati condivisi, effettuare regolarmente copie di backup verificando periodicamente la correttezza dei salvataggi effettuati, nonché l'efficacia delle procedure di ripristino adottate.
  Maggiori dettagli in merito sono reperibili al seguente indirizzo:
  https://www.elettra.eu/activities/it-service/backup-vademecum.html

3.2.1 Regole per la scelta della password

La password viene gestita attraverso il sistema VUO (https://vuo.elettra.eu) e deve rispettare le regole di composizione indicate nell'apposita pagina di cambio password del VUO di seguito riportate:

- Per creare la password è possibile utilizzare fino a un massimo di 64 caratteri. I caratteri consentiti sono le lettere minuscole e maiuscole [a-zA-Z], i caratteri numerici [0-9] e i caratteri speciali ~ `! @ # $% ^ & * ( ) -_ + = { } [ ] | \ ; : " < > , . / ? .
- Se la password è lunga almeno 12 (dodici) caratteri, può contenere solo lettere minuscole [a-z].
- Se la password è più corta di 12 (dodici) caratteri allora deve essere lunga almeno 8 (otto) caratteri e deve contenere:
  - un minimo di 1 lettera minuscola [a-z]
  - almeno 1 lettera maiuscola [A-Z]
  - un minimo di 1 carattere numerico [0-9]
  - un minimo di 1 carattere speciale: ~ `! @ # $% ^ & * ( ) -_ + = { } [ ] | \ ; : " < > , . / ?
- La password non deve contenere il proprio nome, cognome, indirizzo email o data di nascita.
- In ogni caso evita di utilizzare schemi comuni come 12345678 o qwerty e schemi di caratteri ripetuti.

La password inoltre deve essere modificata periodicamente secondo le indicazioni fornite dallo stesso VUO ossia almeno ogni 6 (sei) mesi e in caso di trattamento di dati sensibili almeno ogni 3 (tre) mesi.

Gli utenti non devono comunicare a nessuno le proprie password né concedere ad altri l'uso del proprio account, del quale sono pienamente responsabili.

È necessario:

- evitare di usare la stessa password su sistemi diversi;
- utilizzare l'autenticazione a due fattori (2FA) o sistemi CAPTCHA se previsti dal sistema o servizio utilizzato;
- utilizzare eventualmente sistemi di gestione delle password che salvano le singole password utilizzando la crittografia e protetti da una password principale detta "Master password";
- evitare di utilizzare script/programmi che contengano la password di accesso ad un qualsiasi computer riportate in chiaro (senza alcuna forma di protezione).

3.2.2 Regole per l'assegnazione degli indirizzi di rete (IP)

Per richiedere la connessione alla rete dati di Elettra di una qualunque apparecchiatura, va compilato un apposito modulo elettronico reperibile alla voce "Lan Connection Request" della pagina https://www.elettra.eu/it-service/index.html. Dopo la verifica dell'autenticità del richiedente e la valutazione dell'opportunità del collegamento alla rete LAN, l'Attività Sistemi e Servizi ICT provvederà all'assegnazione di un nome e di un indirizzo di rete (indirizzo IP) per

l'apparecchiatura per un periodo determinato e rinnovabile e ne darà comunicazione al richiedente stesso.

La dismissione/cessione dello strumento a cui è stato precedentemente assegnato un indirizzo IP, va segnalata all'Attività Sistemi e Servizi ICT, che provvederà in questo modo a rendere nuovamente disponibile detto indirizzo.

3.2.3 Regole per l'utilizzo di software in Azienda

L'utilizzo di applicativi software è soggetto al possesso di regolare licenza che ne consenta l'uso in ambito aziendale. È inoltre necessario che ciascun utente provveda a registrare e a mantenere aggiornato il database con ogni risorsa di calcolo (hardware e software) in sua dotazione, secondo quando previsto dalla Circolare n. 09/2017 reperibile all'indirizzo:

https://www.elettra.eu/bacheca_docs/azienda/circolare2017_09mz_mycameras_170811.pdf

Il database è accessibile all'indirizzo (https://services.elettra.eu) dopo essersi autenticati e selezionando la funzione MyDevices. Per ciascun sistema (PC, Laptop, etc.) in dotazione sarà possibile indicare i software in esso installati. Istruzioni dettagliate su queste operazioni possono essere reperite nella stessa pagina.

3.2.4 Rete dati e servizi

In generale, senza l'autorizzazione del Gruppo Informatica, è vietato:

- utilizzare strumenti che potenzialmente siano in grado di consentire l'accesso non autorizzato alle risorse di calcolo (ad esempio 'cracker' o software di monitoraggio della rete);
- configurare servizi già messi a disposizione in modo centralizzato, come, ad esempio, DNS (Domain Name Service), DHCP (*Dynamic Host Configuration Protocol*), NTP (*Network Time Protocol*), mail server, FTP (*File transfer Protocol*), HTTP (*World Wide Web*), accesso remoto (*dial-up*);
- effettuare operazioni di routing (instradamento), bridging (connessione di reti diverse), tunneling (far transitare protocolli "esterno o alieno" sulla rete dati);
- intercettare pacchetti sulla rete, utilizzando "sniffer" o software/hardware che siano in grado di analizzare tutti dati in transito sulla rete;
- cablare o collegare apparecchiature alle prese di rete;
- adottare indirizzi di rete e nomi non espressamente assegnati all'utilizzatore dall'Attività Sistemi e Servizi ICT;
- condividere le credenziali di autenticazione (account comuni);
- installare apparecchiature di rete wireless;
- utilizzare modem per l'accesso remoto attraverso la linea telefonica;
- aprire e gestire autonomamente siti Web;
- accedere ai locali e/o agli armadi destinati alle risorse di calcolo ed alle apparecchiature di rete, nonché apportarvi qualsiasi modifica.

3.2.5 Software e dati

È vietata la duplicazione, l'uso non autorizzato, il download e/o l'upload di qualsiasi programma software, file audio (es: mp3, wav, ecc.), video (DivX, mpeg, etc.), immagini o testi quando espressamente indicato dal loro copyright.

È vietato l'uso di software in violazione della licenza d'uso prevista. In particolare è vietato utilizzare qualunque software di cui non si possieda regolare licenza che consenta l'utilizzo in ambito aziendale. Nel caso di prodotti con licenza gratuita è necessario verificare che tale licenza consenta l'uso per scopi aziendali e non solo domestici o privati. È strettamente consigliato consultare sempre l'Attività Sistemi e Servizi ICT prima di acquisire qualsiasi nuova licenza software, anche gratuita.

Nel caso in cui l'Attività Sistemi e Servizi ICT non sia in grado di verificare la liceità dell'uso aziendale di una licenza gratuita o in qualsiasi altro caso di dubbio, si rivolgerà all'Attività Affari Legali e Istituzionali per gli approfondimenti del caso prima di qualsiasi acquisizione di nuova licenza.

È vietato l'uso di software che possa danneggiare le risorse di calcolo e della rete.

È vietato utilizzare programmi potenzialmente pericolosi del tipo Peer-to-Peer (P2P) quali, ad esempio, eMule, BitTorrent, etc. senza preventiva autorizzazione del Gruppo Informatica.

È vietato effettuare copie di file di configurazione di sistemi dei quali non si ha accesso privilegiato.

Per quanto riguarda le problematiche connesse ai dati scientifici si faccia riferimento al documento denominato "Scientific Data Policy" PIOR-SCH-04-rev01EN accessibile anche al link: https://www.elettra.eu/userarea/scientific-data-policy.html.

3.2.6 Posta elettronica

Una casella di posta elettronica nel dominio @elettra.eu viene assegnata a tutto il personale titolare di un rapporto di lavoro subordinato con Elettra di durata superiore ai 6 (sei) mesi.
È possibile assegnare caselle di posta elettronica anche per periodi inferiori nel caso in cui esistano opportune motivazioni. La valutazione verrà effettuata dall'Attività Risorse Umane.
La casella di posta elettronica viene attivata a decorrere dal primo giorno di contratto e disattivata al termine dell'ultimo giorno. Una volta disattivata, essa continuerà a ricevere mail per ulteriori 6 (sei) mesi, ma non sarà possibile accedervi. Allo scadere di questo periodo, essa verrà eliminata definitivamente con la conseguente cancellazione di tutti i messaggi in essa contenuti.
Alcuni giorni prima dell'inizio del periodo di 6 (sei) mesi di inaccessibilità l'utente è tenuto ad impostare un messaggio di risposta automatica indicando un eventuale nuovo contatto e a chi inoltrare richieste di carattere professionale (Responsabile di Attività, Coordinatore di Gruppo, referente scientifico, etc.). Qualora il messaggio non venga impostato, ne verrà configurato uno d'ufficio che informerà il mittente che la casella di posta elettronica non è più presidiata.
È vietato inoltrare automaticamente i messaggi di posta elettronica aziendali verso caselle di posta elettronica esterne ad Elettra.

È vietato configurare altri servizi esterni di posta elettronica affinché accedano alla casella di posta aziendale.
La casella di posta elettronica deve essere utilizzata per lo scambio di messaggi ad esclusivo uso professionale ed eventualmente utilizzata per registrarsi su siti, mailing list e servizi di esclusivo interesse istituzionale e per fini professionali.
Gli amministratori di sistema incaricati potranno svolgere attività di monitoraggio del traffico di posta elettronica esclusivamente per finalità di verifica di anomalie di funzionamento, di mitigazione di attacchi malevoli o di individuazione di utilizzo illecito del servizio.
I sistemi automatici di mitigazione del rischio di attacchi informatici analizzeranno il contenuto dei messaggi e la tipologia degli allegati al fine di individuare virus o messaggi contenenti informazioni o collegamenti malevoli. Il comportamento dei sistemi automatici potrà essere personalizzato dal singolo utente secondo quanto descritto nelle apposite pagine web pubblicate nella Intranet aziendale.

3.2.7 Lavoro agile

La modalità di lavoro agile può essere effettuata sia utilizzando le risorse personali che quelle messe a disposizione dell'azienda con opportuni accorgimenti.
L'Azienda non fornisce connessione di rete al lavoratore in modalità di lavoro agile, che deve quindi provvedervi personalmente. Le caratteristiche della connessione devono essere adeguate a fornire la prestazione lavorativa in base agli incarichi assegnati. La rete wireless deve essere altresì protetta almeno da una chiave di tipo WPA2.
La Società non è tenuta a fornire, oltre alla dotazione di base, alcun accessorio aggiuntivo di nuova acquisizione (monitor, stampanti, toner, inchiostri, alimentatori addizionali, etc.).

Personal Computer Privato

Qualora si utilizzi una risorsa o un personal computer privato, non vi deve mai essere salvato alcun dato o documento aziendale poiché potrebbe andare in mano a soggetti non autorizzati. Inoltre su un personal computer privato non è in alcun modo possibile installare software con licenza aziendale a meno che non sia prevista esplicitamente questa possibilità dal produttore e che vi sia anche l'autorizzazione della Società. Il personale del Gruppo Informatica non effettuerà direttamente alcun intervento di assistenza hardware o software sui computer privati.
Di seguito vengono elencate le prescrizioni da rispettare nel caso di utilizzo di un personal computer privato per il lavoro agile:

- È vietato:
  - installare o utilizzare software che possa generare traffico illecito in particolar modo se si utilizza la connessione VPN;
  - utilizzare sistemi di salvataggio delle password che non prevedano la protezione delle singole password utilizzando la crittografia e siano a loro volta protetti da una password principale o "Master password";

- È altresì obbligatorio:
  - installare un antivirus approvato dal Gruppo Informatica e verificare che sia sempre operativo;
  - segnalare qualsiasi malfunzionamento hardware o software al Gruppo Informatica anche attraverso il sistema VUO (vuo.elettra.eu) sezione

"Richieste di intervento IT" fermo restando che non verranno effettuati dal Gruppo Informatica interventi su risorse private;
- mantenere i file inerenti all'attività professionale su sistemi di immagazzinamento dati condivisi, remoti che sono sottoposti ad adeguate politiche di backup (Elettra Drive, online4, gitlab, etc.);
- attivare la connessione VPN quando ci si trovi ad operare utilizzando reti non protette (locali pubblici, aeroporti, spazi all'aperto, stazioni ferroviarie, etc.).

Personal Computer Aziendale

Qualora si utilizzi una risorsa aziendale, è vietato concederne l'utilizzo a terze parti (familiari, amici ed altre persone che possano frequentare i luoghi in cui viene svolta l'attività lavorativa in modalità di lavoro agile) ed è inoltre vietato lasciare la risorsa incustodita in luoghi pubblici.

Di seguito vengono elencate le prescrizioni da rispettare durante lo svolgimento dell'attività lavorativa in modalità di lavoro agile utilizzando un personal computer aziendale:

- È vietato:
  - installare software senza regolare licenza fornita dalla Società;
  - installare software non inerente all'attività professionale e in genere agli incarichi assegnati;
  - salvare file non inerenti l'attività professionale e in genere agli incarichi assegnati;
  - utilizzare il dispositivo per attività non inerenti al proprio incarico;
  - intervenire sull'hardware in dotazione senza una specifica autorizzazione del Gruppo Informatica;
  - modificare la configurazione del sistema operativo;
  - installare o utilizzare software che possa generare traffico illecito in particolar modo se si utilizza la connessione VPN;
  - utilizzare sistemi di salvataggio delle password che non prevedano la protezione delle singole password utilizzando la crittografia e siano a loro volta protetti da una password principale o "Master password";

- È altresì obbligatorio:
  - installare un antivirus approvato dal Gruppo Informatica e verificare che sia sempre operativo;
  - segnalare qualsiasi malfunzionamento hardware o software al Gruppo Informatica anche attraverso il sistema VUO (vuo.elettra.eu) sezione "Richieste di intervento IT";
  - mantenere i file inerenti all'attività professionale su sistemi di immagazzinamento dati condivisi, remoti che sono sottoposti ad adeguate politiche di backup (Elettra Drive, online4, gitlab, etc.);
  - attivare la connessione VPN quando ci si trovi ad operare utilizzando reti non protette (locali pubblici, aeroporti, spazi all'aperto, stazioni ferroviarie, etc.).

Divieti e obblighi sono mirati esclusivamente alla protezione dei dati aziendali e al rafforzamento delle misure di sicurezza. Nel rispetto di quanto previsto dal GDPR e dall'art. 4 dello Statuto dei Lavoratori e s.m.i., le attività di monitoraggio sul corretto

utilizzo delle apparecchiature hardware e software saranno condotte a campione o in seguito ad episodi che si configurano come incidenti di sicurezza. Detto monitoraggio avrà come unico fine: garantire la sicurezza dei dati, la continuità aziendale e la prevenzione degli illeciti. I controlli del rispetto di prescrizioni e divieti verranno effettuati dal solo personale autorizzato. Le eventuali violazioni verranno segnalate al Coordinatore di Gruppo competente, all'Attività Risorse Umane e nei casi più gravi alle autorità competenti e comporteranno la revoca dell'autorizzazione allo svolgimento del lavoro agile.

3.2.8 Altre prescrizioni

È vietato effettuare interventi hardware sulle risorse di calcolo e rete di Elettra, comprese quelle ricevute personalmente in affidamento (PC, stampanti, etc.), senza una specifica autorizzazione del Gruppo Informatica.

È inoltre vietato intraprendere azioni allo scopo di:

- degradare le risorse del sistema;
- impedire l'accesso alle risorse ad utilizzatori autorizzati;
- allocare arbitrariamente risorse superiori a quelle precedentemente autorizzate;
- accedere a risorse di calcolo, sia di Elettra che di terze parti, violando le misure di sicurezza.

3.2.9 Bring Your Own Device (BYOD)

La pratica Bring your own device (BYOD) - chiamata anche bring your own technology (BYOT), bring your own phone (BYOP) e bring your own PC (BYOPC), che in italiano si traduce con "*porta il tuo dispositivo*, *porta la tua tecnologia*, *porta il tuo telefono* e *porta il tuo PC"* è consentita purchè si seguano le stesse indicazioni riportate per l'utilizzo del Personal Computer privato nel paragrafo relativo al lavoro agile.

3.3 Sanzioni

L'inosservanza della presente Procedura potrà essere sanzionata come previsto dal Codice disciplinare aziendale e dal Codice di comportamento di Elettra. Ogni violazione sarà segnalata al Responsabile dell'Attività Risorse Umane e, nei casi in cui si ravvisino estremi di reato, alle Autorità competenti.
In ogni caso, le attività non conformi alle regole contenute nel presente documento che diano luogo a violazioni della sicurezza delle risorse di calcolo e rete sono vietate e daranno pertanto luogo alla sospensione o alla revoca dell'accesso alle risorse stesse.
In caso di violazione delle prescrizioni previste dal presente disciplinare che abbia comportato un danno patrimoniale o non patrimoniale alla Società, il dipendente che si sia reso responsabile della violazione sarà tenuto al risarcimento del predetto danno.

3.4 Deroghe

Qualora vi sia una documentata necessità di eventuali deroghe alle indicazioni riportate nel seguente documento, queste vanno autorizzate esplicitamente dall'Amministratore Delegato. Le richieste di deroga vanno sottoposte, corredate da adeguata documentazione che ne motivi la necessità, al Gruppo Informatica che provvederà ad effettuare un'analisi dei rischi informatici collegati e a sottoporre la documentazione raccolta all'Amministratore Delegato per le valutazioni del caso.

4 Link utili

Il presente Disciplinare Tecnico ed ogni futuro aggiornamento è anche disponibile, in forma elettronica, al seguente indirizzo, sotto il processo “Proteggere i dati”:
https://www.elettra.eu/utilities/processi.html

4.1 Pagine dell'Attività Sistemi e Servizi ICT

Le pagine relative all’ Attività Sistemi e Servizi ICT sono consultabili all’indirizzo:
https://www.elettra.eu/it-service/index.html

4.2 Pagine del Garante per la protezione dei dati personali

https://www.garanteprivacy.it

4.3 Pagine dell'organizzazione della privacy a Elettra

Le pagine relative all’ organizzazione della privacy a Elettra - Sincrotrone Trieste S.C.p.A. sono consultabili all’indirizzo:
https://www.elettra.eu/public/privacy/privacy.html

4.4 Dati relativi alla proprietà intellettuale a Elettra

Per informazioni riguardanti il trattamento dei dati relativi alla proprietà intellettuale, fare riferimento all’Attività Industrial Liaison Office (ILO):
https://ilo.elettra.eu