Linee Guida

Disciplinare Tecnico Interno sull'utilizzo delle risorse di calcolo e rete

0 Indice

0.1 Emissione del documento

Questo documento ha seguito il seguente iter di ufficializzazione:

• Redazione:	Euro Cocolo (Referente aziendale per la privacy e la protezione dei dati) con la collaborazione di Andrea Crivelli (Attività Risorse Umane), Patrizia Fiore (Attività Affari Legali ed Istituzionali), Marco Lonza	*Redazione*

(Gruppo Informatica) e Paolo Michelini (Attività Servizio Informatico)

- Approvazione: Alfonso Franciosi (Amministratore Delegato)
- Verifica: Mauro Zambelli (Responsabile Sistema di Gestione)

1 Scopo e campo di applicazione

I sistemi informatici, intesi come calcolatori, programmi applicativi, reti di trasmissione dati, eccetera, rivestono oggi un ruolo basilare nello svolgimento di ogni attività lavorativa.
L'estrema diffusione di simili risorse all'interno di Sincrotrone Trieste S.C.p.A. (di seguito indicata come "ST"), 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 a: dipendenti, collaboratori, partner, utenti delle linee di luce, associati, ospiti, dottorandi, borsisti, laureandi, specializzandi, stagisti, di seguito indicati come "personale", è una misura di sicurezza indispensabile per:

- favorire il massimo livello di supporto alle attività del laboratorio;
- 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.

Posto che l'utilizzo delle risorse informatiche deve in ogni caso ispirarsi al principio della diligenza e della correttezza, ST ha adottato il presente Disciplinare Tecnico Interno, 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 ST intende prevenire comportamenti, anche inconsapevoli, che possano dare origine a rischi o minacce per la sicurezza dei dati.

2 Responsabilità

Le attività di configurazione, amministrazione e manutenzione delle risorse di calcolo e rete di proprietà ST 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 alla pagina: Organigramma Privacy della Sincrotrone Trieste S.C.p.A. della sezione http://www.elettra.trieste.it/Privacy

3 Riferimenti

3.1 Riferimenti esterni

Il presente Disciplinare Tecnico Interno viene adottato in conformità ed ottemperanza alla 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"*; del Decreto Legislativo n. 196 dd. 23 giugno 2003, recante *"Codice in materia di protezione dei dati personali"* (di seguito anche indicato come "Codice"); e in ottemperanza alle indicazioni contenute nella 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"*.

3.2 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 ST.

3.2.1 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 (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 apparati e servizi di rete cablata e/o wireless; • gli applicativi software acquistati e/o distribuiti da ST; • i servizi informatici o di rete, forniti in modo centralizzato da ST.
3.2.2 Accesso ad internet	L'accesso ad internet dalla rete locale di ST avviene attraverso la Rete Italiana dell'Università e della Ricerca Scientifica, denominata comunemente "Rete GARR". L'uso di detta rete, da parte di ST 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 http://www.garr.it/reteGARR/aup.php?idmenu=collegare. 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 ST 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. E' pertanto rimesso alla correttezza dell'utente il buon utilizzo dell'accesso risultando il medesimo personalmente responsabile nel caso in cui adotti un comportamento scorretto.
3.2.3 Amministratore di sistema e/o	Per "amministratore di sistema e/o di rete" si intende in generale la figura professionale, in ambito informatico, in possesso delle competenze necessarie, finalizzata alla gestione e manutenzione

di rete	hardware e software di sistemi di elaborazione, reti di trasmissione dati, basi dati. L'elenco completo degli Amministratori di sistema e/o di rete è disponibile e consultabile alla pagina Organigramma Privacy della Sincrotrone Trieste S.C.p.A. della sezione http://www.elettra.trieste.it/Privacy.
3.2.4 Credenziali di autenticazione	Per "credenziali di autenticazione" si intendono 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).
3.2.5 Dato personale	Per "dato personale" si intende "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" [Art. 4, comma 1) lett. b) del "Codice"].
3.2.6 Dato sensibile	Per "dato sensibile" si intendono "i dati personali idonei a rivelare 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" [*Art. 4, comma 1) lett. d) del "Codice"*].
3.2.7 Incaricati del trattamento	Per "incaricati del trattamento dei dati" si intendono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.
3.2.8 Trattamento	Per "trattamento" si intende qualunque operazione o complesso di operazioni, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.
3.2.9 Titolare del trattamento	Per "titolare" del trattamento si intende "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza" " [*Art. 4, comma 1) lett. f) del Codice*]. Titolare del trattamento di ST è: **Sincrotrone Trieste S.C.p.A. di interesse_nazionale - Strada Statale 14, km 163,5 in AREA Science Park - 34149 Basovizza (Trieste).**
3.2.10 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 ST, senza possedere accessi privilegiati alle risorse stesse.

4 Modalità operative

Il personale che utilizza le risorse di calcolo e di rete di proprietà di ST 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.

4.1 Responsabilità, diritti e doveri

4.1.1 Datore di lavoro / titolare del trattamento

Secondo quanto prescritto dal Garante per la protezione dei dati personali, compete ai datori di lavoro assicurare la funzionalità ed il corretto impiego delle risorse di calcolo e di rete utilizzate dai propri collaboratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa [*All. B. del Codice - "Disciplinare tecnico in materia di misure minime di sicurezza"*].

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 saltuarie od occasionali:

- 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, sw, ...);
- 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 personal computer, 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 effettuati.

ST 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 possono essere automaticamente registrate in forma elettronica, 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".

4.1.2 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 ST e, più in generale, secondo quanto disposto dalle normative di legge vigenti.

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

4.1.3 Utenti

Le risorse di calcolo e rete di proprietà di ST, 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'Allegato B) del Codice *"Disciplinare Tecnico in Materia di Misure Minime di Sicurezza"* 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 a cui esse possono accedere e dei dati su di esse memorizzati (Rif. captolo "Divieti" del presente Disciplinare Tecnico).

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

È consentito il collegamento alla rete locale di ST di computer non appartenenti a ST solo mediante specifica e preventiva autorizzazione da parte del Coordinatore del Gruppo di appartenenza o dell'Amministratore delegato di ST. Su detti computer è in ogni caso vietata l'installazione di software con licenza d'uso registrata a nome di ST.

Non è consentito il collegamento alla rete locale di ogni altro tipo di apparecchiature non appartenenti ad ST, se non espressamente autorizzato dall'Amministratore Delegato di ST.

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.
In caso di trattamento di dati personali e/o sensibili, gli utenti sono tenuti ad

attenersi alle misure minime di sicurezza dettate dal decreto legislativo 30 giugno 2003, n. 196 consultabile anche dalla pagina http://www.elettra.trieste.it/Privacy.

Gli utenti sono in ogni caso tenuti a segnalare prontamente al responsabile 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 sua prolungata assenza o impedimento che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

4.2 Misure minime di sicurezza

ST, in qualità di titolare del trattamento deve, secondo quanto disposto dal *"Codice in materia di protezione dei dati personali"*, provvedere ad adottare opportune misure di sicurezza a protezione dei dati e dei relativi sistemi con i quali viene effettuato il trattamento. (Artt. 31, 33, 34, 35 del *"Codice"*).

Gli utenti sono tenuti ad osservare le seguenti misure minime di sicurezza:

- 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 provvedere regolarmente all'aggiornamento delle cosiddette "definizioni di virus". L'Attività Servizio Informatico è tenuto 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 Servizio Informatico si impegna a fornire il massimo supporto informativo e pratico;
- utilizzare un salvaschermo con password, attivabile automaticamente dopo un tempo prefissato non superiore ai 30 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 Servizio Informatico.

4.2.1 Regole per la scelta della password

La password deve essere composta da almeno otto caratteri (lettere maiuscole e minuscole, numeri e caratteri speciali quali _ & ^ % $ #); essa non deve contenere riferimenti agevolmente riconducibili all'utilizzatore (parole del dizionario di qualunque lingua, nomi propri o geografici, date di nascita o di anniversari, ecc.) ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili la password deve essere modificata almeno ogni 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.

Si consiglia inoltre di:
- evitare di usare la stessa password su sistemi diversi;
- non utilizzare script/programmi che contengano la password di accesso ad un qualsiasi computer.

4.2.2 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 http://www.elettra.trieste.it/it. Dopo la verifica di autenticità del richiedente, l'Attività Servizio Informatico provvederà all'assegnazione di un nome e di un indirizzo di rete (indirizzo IP) per l'apparecchiatura 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 Servizio Informatico, che provvederà in questo modo a rendere nuovamente disponibile detto indirizzo.

4.3 Divieti

L'inosservanza delle presenti Linee Guida potrà essere sanzionata come previsto dal regolamento disciplinare aziendale.
Ogni violazione sarà segnalata al Responsabile dell'Area 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 nella sicurezza delle risorse di calcolo e rete sono vietate e daranno pertanto luogo alla sospensione o alla revoca dell'accesso alle risorse stesse.

4.3.1 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, bridging, tunneling*;
- intercettare pacchetti sulla rete, utilizzando "sniffer" o software/hardware analoghi;
- cablare o collegare apparecchiature alle prese di rete;
- adottare indirizzi di rete e nomi non espressamente assegnati all'utilizzatore dall'Attività Servizio Informatico;
- 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 del Gruppo Informatica, nonché apportarvi qualsiasi modifica.

4.3.2 Software e dati

E` 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 soggetti a copyright.

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

E` vietato utilizzare programmi potenzialmente pericolosi del tipo Peer-to-Peer (P2P) quali, ad esempio, eMule, BitTorrent, ecc. o IRC (Internet Relay Chat) quali, ad esempio, mIRC, Xchat, Gaim, ecc., senza preventiva autorizzazione del Servizio Informatico.

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

4.3.3 Altro

È vietato effettuare interventi hardware sulle risorse di calcolo e rete di ST, comprese quelle avute personalmente in affidamento (personal computer, stampanti, ecc.), 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 ST che di terze parti, violandone le misure di sicurezza.

5 Link utili

Il presente Disciplinare Tecnico Interno ed ogni futuro aggiornamento è anche disponibile, in forma elettronica, al seguente indirizzo:
http://www.elettra.trieste.it/intranet/staff_guide/

5.1 Pagine dell'Attività Servizio Informatico

Le pagine relative all' Attività Servizio Informatico sono consultabili all'indirizzo http://www.elettra.trieste.it/it

5.2 Pagine del Garante per la protezione dei dati personali

http://www.garanteprivacy.it

5.3 Pagine dell'organizzazione della privacy in ST

Le pagine relative all' organizzazione privacy in Sincrotrone Trieste S.C.p.A. sono consultabili all'indirizzzo http://www.elettra.trieste.it/Privacy

5.4 Dati relativi alla proprietà intellettuale in ST

Per informazioni riguardanti il trattamento dei dati relativi alla proprietà intellettuale, fare riferimento all'Attività Industrial Liaison Office (ILO):

http://ilo.elettra.trieste.it