



FONDAZIONE  
SVILUPPO  
CA' GRANDA

# **REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATIVI**

Approvato dal Consiglio di amministrazione in data 20 aprile 2017



## **REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATIVI**

### **Art. 1**

#### **Scopo ed ambito di applicazione**

1. Il presente documento (di seguito "Regolamento") definisce le finalità e le modalità di utilizzo dei sistemi informativi messi a disposizione da Fondazione Sviluppo Ca' Granda (di seguito "Fondazione Sviluppo").
2. Il Regolamento si applica ai dipendenti e a tutti coloro che hanno accesso ai sistemi informativi della Fondazione (di seguito anche solo "Utenti").

### **Art. 2**

#### **Definizioni**

1. Salva diversa specifica indicazione, nel presente Regolamento i seguenti termini ed espressioni con iniziale maiuscola avranno il significato che nel seguito è ad essi attribuito:
  - **"Credenziali di Autenticazione"**: l'insieme degli elementi identificativi di un Utente e consistono in un codice per l'identificazione ("User id") associato a una parola chiave riservata ("Password");
  - **"Dato informatico"** (o **"Dato"**): qualunque rappresentazione di fatti, informazioni o concetti, in forma idonea per l'elaborazione o la conservazione con un Sistema Informatico, incluso un programma atto a consentire ad un sistema informatico lo svolgimento di funzioni;
  - **"PC"**: personal computer fisso o portatile;
  - **"Personale Tecnico"**: Amministratori di sistema, operatori di sistema, sistemisti, sviluppatori di software, tecnici che effettuano manutenzione hardware e, in generale, tutti coloro che - per esigenze di manutenzione, gestione, monitoraggio e implementazione - operano sul Sistema Informatico;
  - **"Personale ICT"**: personale incaricato che opera presso l'Ufficio Servizi generali di Fondazione Sviluppo;
  - **"Postazione di Lavoro"**: postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni aziendali;
  - **"Server"**: elaboratore dedicato alla fornitura di risorse e servizi per altri computer, detti "client", connessi fisicamente tra loro in rete;
  - **"Servizi di rete"**: servizi forniti dal Server ed in particolare la posta elettronica, la navigazione Internet, le cartelle condivise, le stampanti condivise e gli applicativi aziendali;
  - **"Sistema informatico"**: qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, che, in base ad un programma, consente l'elaborazione automatica di Dati;
  - **"Spamming"**: l'invio di messaggi indesiderati;
  - **"Utente"**: ogni dipendente o chiunque sia stato autorizzato all'utilizzo o all'accesso ai sistemi informatici aziendali;



- **“Virus”**: software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente.

### **Art. 3**

#### **Utilizzo dei PC**

1. I PC ed ogni connesso apparecchio sono strumenti di lavoro.
2. L'utilizzo dei PC è consentito solo per l'esercizio delle mansioni assegnate a ciascun Utente, e comunque nel rispetto dei limiti previsti dal Regolamento e dalla normativa applicabile. Ogni utilizzo diverso, o comunque non inerente all'attività lavorativa, è vietato.
3. Per utilizzare il PC l'Utente deve inserire le proprie Credenziali di Autenticazione.
4. L'uso di ciascun PC è strettamente personale; pertanto, è fatto divieto agli Utenti di:
  - a) lasciare incustodita ed accessibile, e/o comunque consentire l'utilizzo della propria Postazione di Lavoro da parte di persone non autorizzate;
  - b) comunicare a terzi, o comunque consentire direttamente o indirettamente a terzi la conoscenza delle proprie Credenziali di Autenticazione, fatto salvo quanto stabilito nel Regolamento;
  - c) utilizzare Credenziali di Autenticazione di altri Utenti, nemmeno se fornite volontariamente, fatto salvo quanto stabilito nel Regolamento.
5. Non è consentito agli Utenti:
  - a) in assenza di un'esplicita autorizzazione del Personale ICT, la modificazione o l'alterazione delle configurazioni impostate sul proprio PC;
  - b) l'utilizzo di strumenti hardware o software atti a intercettare, falsificare, alterare, copiare o sopprimere il contenuto di comunicazioni e/o strumenti informatici;
  - c) l'installazione, l'assemblaggio, ovvero l'utilizzo, con il proprio PC, di software, hardware ovvero strumenti o mezzi di comunicazione (ad esempio modem) né di altri apparecchi (ad esempio masterizzatore, lettore MP3, chiavette USB, etc.), così come di accessori, dispositivi, applicazioni o programmi di qualsivoglia genere, anche di proprietà dell'Utente, senza l'esplicita autorizzazione scritta del Personale ICT;
  - d) trasferire o creare sul proprio PC file, di qualunque genere e tipo, che non abbiano diretta attinenza con le mansioni dell'Utente e che non siano necessari o funzionali al relativo espletamento;
  - e) trasferire sul proprio PC tutti i file di provenienza incerta o sospetta, sia essa interna o esterna a Fondazione Sviluppo, ancorché attinenti all'attività lavorativa. Prima di essere aperti devono essere segnalati o fatti controllare del Personale ICT, che ne potrà anche non autorizzare l'utilizzo;
  - f) copiare, salvare su supporti informatici esterni, comunicare o divulgare file o dati informatici contenuti su PC, elaborati dagli stessi Utenti o da terzi, comunque accessibili all'interno dei PC o grazie ad essi, se non nell'interesse di Fondazione Sviluppo; è parimenti vietato agli Utenti di permettere a terzi di effettuare tali attività;
  - g) lasciare il PC acceso al termine dell'orario di lavoro. L'Utente dovrà spegnere il proprio PC al termine della prestazione giornaliera o comunque prima di lasciare la sede di lavoro o in caso di assenze giornaliere prolungate dalla postazione di lavoro (in caso di assenza non prolungata potrà essere utilizzata la funzione di standby del PC);
6. Con particolare riferimento ai PC portatili, si specifica inoltre quanto segue:



- a) gli Utenti sono responsabili della custodia e della cura necessaria dei PC portatili;
  - b) qualora dovessero rendersi necessarie eventuali riparazioni, sarà cura dell'Utente avvisare tempestivamente di ciò il Personale ICT. Fondazione Sviluppo si riserva di valutare di volta in volta la natura delle riparazioni e ove le stesse fossero conseguenti ad incuria o negligenza, i relativi costi saranno a carico dell'Utente;
  - c) in caso di smarrimento o furto sarà cura dell'Utente avvisare immediatamente Fondazione Sviluppo e denunciare l'accaduto all'Autorità di Pubblica Sicurezza;
  - d) qualora, in qualsiasi momento, Fondazione Sviluppo ravvisasse delle manchevolezze da parte dell'Utente nella corretta gestione ed utilizzo del PC portatile, sarà facoltà di Fondazione Sviluppo revocare l'assegnazione dello stesso;
  - e) all'atto della cessazione del rapporto di lavoro, l'Utente sarà tenuto a restituire il PC portatile, nelle medesime condizioni, sia sotto il profilo hardware che sotto il profilo software, in cui lo ha ricevuto, fermo restando che nessuna formattazione sarà consentita.
7. Fondazione Sviluppo rende noto che il Personale ICT e/o il Personale Tecnico è autorizzato a compiere interventi sul Sistema Informatico volti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'azienda, si applica anche in caso di assenza prolungata od impedimento dell'Utente.
8. Il Personale ICT e/o il Personale Tecnico ha la facoltà di collegarsi e visualizzare in remoto il desktop delle Postazioni di Lavoro al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro Virus, spyware, malware, etc. L'intervento viene effettuato previa richiesta dell'Utente o, in caso di necessità, a seguito della rilevazione tecnica di anomalie/malfunzionamenti del Sistema Informatico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

#### **Art. 4**

#### **Gestione ed assegnazione delle credenziali di autenticazione**

1. Le Credenziali di Autenticazione per l'accesso PC vengono assegnate dal Personale ICT, previa autorizzazione del Direttore generale.
2. Le Credenziali di Autenticazione consistono in un codice per l'identificazione dell'utente ("User id"), assegnato dal Personale ICT, associato ad una parola chiave ("Password") riservata che dovrà venir custodita dall'Utente con la massima diligenza e non divulgata.
3. La Password, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'Utente.
4. È necessario procedere alla modifica della Password a cura dell'Utente al primo utilizzo e, successivamente, almeno ogni sei mesi (ogni tre mesi nel caso invece di trattamento di *dati sensibili*<sup>1</sup> attraverso l'ausilio di strumenti elettronici).

---

<sup>1</sup> Trattamento di categorie particolari di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici



#### **Art. 5**

##### **Accesso ed utilizzo dei servizi di rete**

1. Per accedere ai Servizi di Rete l'Utente deve essere in possesso di Credenziali di Autenticazione, assegnati dal Personale ICT previa autorizzazione del Direttore generale.
2. È fatto il più assoluto divieto di accedere ai Sistemi di Rete con Codici di Autenticazione diversi da quelli assegnati.
3. Le cartelle utenti presenti nei Server di Fondazione Sviluppo (di seguito "Cartelle Utenti") sono aree di condivisione di informazioni strettamente professionali e riservate e non possono in alcun modo essere utilizzate per scopi diversi dall'esercizio delle proprie mansioni. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere inserito, nemmeno per brevi periodi, nelle Cartelle Utenti. Sulle Cartelle Utenti vengono svolte regolari attività di amministrazione e backup da parte del Personale ICT e/o del Personale Tecnico. I dati oggetto di backup verranno conservati su adeguati supporti e in luogo sicuro per un periodo adeguato alle necessità. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: o D: interni al PC) non sono soggette a salvataggio da parte del Personale Tecnico e/o del Personale ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.
4. Viene effettuato un backup giornaliero di tutta la documentazione presente sui Server. I dati presenti nei backup non sono in alcun modo modificabili, né tantomeno eliminabili (neppure su esplicita richiesta dell'Utente). Il backup dei dati viene mantenuto per una durata di tempo compatibile con quanto previsto dalla normativa vigente.
5. Il Personale Tecnico e/o Personale ICT può, in qualunque momento, procedere alla rimozione di ogni file o applicazione pericolosa per la sicurezza del Sistema Informatico.
6. È consentito inserire materiale multimediale (foto, video, audio) nelle Cartelle Utenti solo qualora sia pertinente all'attività lavorativa e sia stato acquisito nel rispetto della D.Lgs 196/2003 e s.m.i..
7. Ciascun Utente è tenuto a provvedere periodicamente (almeno ogni tre mesi) alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

#### **Art. 6**

##### **Utilizzo e conservazione dei supporti rimovibili**

1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali e/o sensibili nonché informazioni relative a Fondazione Sviluppo o costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere sottratto, alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti i suddetti dati, ciascun Utente dovrà contattare il Personale ICT e seguire le istruzioni da questo impartite.

---

intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.



3. In ogni caso, i predetti supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
4. È vietato l'utilizzo di supporti rimovibili personali.
5. L'Utente è responsabile della custodia dei supporti e dei dati aziendali ivi contenuti.

#### **Art. 7**

#### **Uso della posta elettronica**

1. La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. L'Utente è responsabile del corretto utilizzo della stessa.
2. È fatto divieto di utilizzare le caselle di posta elettronica per motivi o finalità diverse da quelle strettamente connesse all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare la posta elettronica per:
  - a) l'invio e/o il ricevimento di allegati contenenti immagini, filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
  - b) l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
  - c) la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Personale ICT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
3. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e allegati ingombranti. A tale proposito, il Personale ICT, può fornire supporto per attuare un'apposita archiviazione dei messaggi di posta in modo che risultino accessibili all'Utente stesso e siano contemporaneamente dislocati su appositi server di backup.
4. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Fondazione Sviluppo ovvero contenga documenti da considerarsi riservati deve essere opportunamente protetta da eventuali accessi di soggetti non autorizzati.
5. È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (posta, posta certificata...), devono essere firmate dal Direttore generale.
6. Ciascun Utente è tenuto a porre la massima attenzione nell'aprire i documenti allegati ai messaggi di posta elettronica prima del loro utilizzo ed è fatto divieto di eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti.
7. Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) è dotato di una funzione di invio automatico di messaggi di risposta contenenti l'indirizzo di posta elettronica di un altro soggetto o altre modalità di contatto di Fondazione Sviluppo. In tal caso, la funzionalità deve essere attivata dall'Utente.
8. In caso di necessità, come per esempio nel caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dall'Utente - verrà attivata da parte di Fondazione Sviluppo.
9. Sarà comunque consentito al superiore gerarchico dell'Utente o, comunque, sentito l'Utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'Utente per ogni ipotesi in cui si renda necessario (a titolo esemplificativo, nel caso di mancata attivazione della funzionalità





di cui al precedente punto 7, ovvero nel caso di assenza non programmata di cui al precedente punto 8).

10. Il Personale ICT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 7 dell'art. 3.
11. In caso di cessazione, per qualsivoglia ragione e/o causa, del rapporto di lavoro e/o di collaborazione e/o altro in essere con Fondazione Sviluppo, l'Utente autorizza sin d'ora Fondazione Sviluppo ad accedere alla propria casella di posta elettronica al fine di predisporre la Postazione di Lavoro per un nuovo Utente ed archiviare (in forma cartacea e/o elettronica) le comunicazioni inerenti l'attività lavorativa. L'utilizzo dell'account verrà mantenuto attivo per un periodo di tempo necessario e sufficiente ad informare soggetti terzi che abbiano rapporti con Fondazione Sviluppo al fine di garantire la continuità dell'attività lavorativa.

#### **Art. 8**

##### **Navigazione in internet**

1. Il PC assegnato all'Utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, è fatto divieto all'Utente di:
  - a) caricare ("upload") o scaricare ("download") software, nonché l'utilizzo di documenti provenienti da siti web o http (immagini, filmati e musica), se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il Personale ICT);
  - b) effettuare transazioni finanziarie, ivi comprese le operazioni di remote banking, acquisti on-line e simili;
  - c) registrarsi a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
  - d) partecipare a Forum non professionali, utilizzare chat line (esclusi gli strumenti autorizzati), bacheche elettroniche e registrarsi in guest books anche utilizzando pseudonimi (o nicknames).
2. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, Fondazione Sviluppo ha adottato uno specifico sistema di blocco o filtro automatico che non consente l'esecuzione di determinate operazioni o l'accesso a determinati siti internet.

#### **Art. 9**

##### **Protezione antivirus**

1. Il Sistema Informatico di Fondazione Sviluppo è protetto da software antivirus aggiornato quotidianamente. Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al Sistema Informatico mediante Virus o altri software aggressivi.
2. Nel caso in cui il software antivirus rilevi la presenza di un Virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso spegnere il computer e segnalare prontamente l'accaduto al Personale ICT.



3. Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un Virus, dovrà essere prontamente consegnato al Personale ICT.

#### **Art. 10**

##### **Utilizzo dei telefoni e delle fotocopiatrici aziendali**

1. Il telefono fisso e/o mobile e le fotocopiatrici aziendali sono strumenti di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentito l'uso per finalità personali o comunque non strettamente inerenti l'attività lavorativa stessa, salva previa autorizzazione del Direttore generale.

#### **Art. 11**

##### **Osservanza delle disposizioni in materia di privacy**

1. Fatto salvo quanto previsto nel Regolamento, l'Utente è tenuto ad attenersi alle disposizioni di cui al D. Lgs. 196/2003 in materia di Privacy e di misure minime di sicurezza.

#### **Art. 12**

##### **Accesso ai dati trattati dall'utente**

1. Fondazione Sviluppo, anche tramite il Personale ICT ovvero Personale Tecnico, potrà effettuare trattamenti di dati su tutti gli Strumenti Informatici per motivi di sicurezza del sistema informatico o più in generale del patrimonio aziendale, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di rilevazione di dati statistici e programmazione di interventi informatici e pianificazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa.

#### **Art. 13**

##### **Inosservanza del Regolamento – sistema sanzionatorio**

1. Il rispetto delle previsioni contenute nel Regolamento costituisce, ai sensi dell'art. 2104 del Codice Civile, un dovere per tutti i dipendenti ed in ogni caso un obbligo contrattuale per gli altri soggetti che accedono ai sistemi informativi aziendali.
2. Nel caso in cui si accerti o si venga a conoscenza di una violazione del Regolamento, Fondazione Sviluppo procede nei confronti dei responsabili delle violazioni, ove si tratti:
  - a) di dipendenti, con provvedimenti disciplinari previsti dal contratto collettivo applicabile;
  - b) di personale in assegnazione temporanea, con segnalazione a Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico per l'assunzione di ogni necessario provvedimento;
  - c) di altri soggetti, ai sensi del contratto e/o comunque di quanto previsto dal codice civile e dalle altre normative.





3. Fatto salvo in ogni caso il diritto di Fondazione Sviluppo di chiedere e ottenere il risarcimento dei danni subiti.

**Art. 14**

**Entrata in vigore**

1. Il Regolamento entrerà in vigore il giorno successivo alla data di approvazione del Consiglio di amministrazione.