REGOLAMENTO INFORMATICO AZIENDALE (per personale esterno)

Versione 0.0
Data di emissione 08/07/2021

Cronologia delle versioni

Versione	Data	Modifica
0.0	08/07/2021	Prima Emissione

Sommario

PARTE PRIMA

1. Ambito di applicazione

Le prescrizioni del presente **Regolamento Informatico Aziendale per il personale esterno** (di seguito "**Regolamento Esterni**") si applicano a tutte le persone (di seguito "**Personale Esterno**") che, a fronte di un contratto di collaborazione formalizzato e sottoscritto, devono prestare la propria attività lavorativa, anche saltuaria, presso Lazio Innova S.p.A. (di seguito "**Lazio Innova**" o "**Azienda**") o, per ragioni connesse all'espletamento del proprio lavoro, risultino comunque autorizzate e abilitate all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche o comunque di supporti informatici aziendali.

Le prescrizioni contenute nel presente **Regolamento Esterni** si aggiungono e integrano le prescrizioni delle "**Linee-guida per il trattamento dei dati personali**" e le specifiche istruzioni che potranno essere in altro modo fornite ai soggetti interessati.

È fatto obbligo a tutto il **Personale Esterno** di adeguarsi a quanto richiesto dal presente **Regolamento Esterni**, in quanto ogni utilizzo o comportamento non conforme ad esso, anche derivante da comportamenti non consapevoli, espone l'*Azienda* ad eventuali danni patrimoniali e/o penali che possono compromettere la sicurezza e l'immagine dell'*Azienda* stessa, risultando così perseguibili nelle sedi proprie (disciplinare, civile e/o penale).

Il **Personale Esterno** è coordinato da specifici **Referenti Aziendali** a cui è tenuto rivolgersi per qualsiasi chiarimento o richiesta nell'applicazione del presente **Regolamento Esterni.**

2. Personal Computer Aziendale

Nel caso in cui l'*Azienda* metta a disposizione del **Personale Esterno** un Personal Computer (PC), fisso o portatile, valgono le prescrizioni che seguono:

a. il PC viene fornito già predisposto e opportunamente configurato per permettere di assolvere alle attività lavorative previste;

b. non è consentito in alcun modo un utilizzo del PC per scopi personali e non è consentita l'archiviazione su di esso di dati personali;

c. non è consentita la modifica delle configurazioni impostate sul PC assegnato né la reinstallazione o alterazione del sistema operativo o di qualsiasi altro software in dotazione né l'installazione di dispositivi di comunicazione/connessione e/o memorizzazione (*modem*/*router*, *hard disk* esterni e simili);

d. non sono consentiti l'installazione e l'uso di *software* diversi da quelli in dotazione, ufficialmente installati e preventivamente autorizzati dall'*Azienda*;

e. è fatto divieto assoluto di formattare o alterare o manomettere o distruggere il PC assegnato o rendere inintelligibili i dati in essi contenuti, tramite qualsiasi processo;

f. il PC deve essere posto in modalità "blocco" in caso di non utilizzo (ad es. assenza breve) e comunque deve essere spento a fronte di assenze prolungate (ad es. uscita serale dall'ufficio);

g. il PC deve essere custodito con cura evitando ogni possibile forma di danneggiamento;

h. nel caso di PC Portatile, questo deve essere custodito con la massima diligenza, in particolare fuori dai locali aziendali e durante gli spostamenti, adottando tutte le cautele necessarie per evitare danni o sottrazioni di dati, documenti e informazioni. Nel caso di perdita, smarrimento o furto, deve avvertire immediatamente il **Referente Aziendale** e, qualora ne ricorrano le circostanze, deve immediatamente denunciare l'evento alle Forze dell'Ordine.

i. il PC portatile deve essere utilizzato esclusivamente dall'assegnatario.

In caso di necessità di utilizzare un *software* differente da quello in dotazione o di disporre di una configurazione diversa per il PC assegnato, il **Personale Esterno** deve rivolgersi al proprio **Referente Aziendale** che, se del caso, provvede ad inoltrare specifica richiesta utilizzando l'apposita funzione nell'ambito del ***Servizio di Supporto Utenti***.

Qualora il **Personale Esterno**, per necessità tecniche, riceva il profilo di **Amministratore Locale** del proprio PC, non deve utilizzare tale abilitazione per apportare modifiche alla configurazione o per installare/disinstallare software, in quanto tale profilo deve essere inteso unicamente come un'abilitazione concessa per permettere l'esecuzione delle applicazioni e non per la gestione del PC stesso.

L'*Azienda* si riserva il diritto di sospendere l'utilizzo del PC qualora non sia più necessario all'esecuzione delle attività previste, al termine del rapporto contrattuale o a fronte di un utilizzo non conforme al presente **Regolamento Esterni**. In tutti questi casi è fatto obbligo al **Personale Esterno** di procedere immediatamente alla restituzione del PC assegnato.

Al fine di garantire la funzionalità, la sicurezza e la salvaguardia del sistema stesso o per esigenze tecniche o manutentive (ad esempio aggiornamento, sostituzione, implementazione di programmi, manutenzione *hardware*, ecc.), personale tecnico con qualifica di "Amministratore di Sistema" può dover effettuare interventi sul PC. Detti interventi potranno anche comportare l'accesso, in caso di effettiva necessità, ai dati trattati da ciascuno, nonché la verifica sui siti *internet* acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività, si applica anche in caso di prolungata assenza o impedimento, in caso di effettiva necessità. Tali azioni saranno improntate su principi di gradualità e necessità, prediligendo caso per caso azioni che non comportino trattamenti di dati, se non strettamente necessari.

Al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, *spyware*, *malware*, ecc., personale tecnico con qualifica di "Amministratore di Sistema" può avere la necessità di collegarsi e visualizzare da remoto il *desktop* del PC. L'intervento viene effettuato ordinariamente previa comunicazione al Personale Esterno che deve autorizzarlo. In caso di oggettiva necessità – e cioè a seguito di problematiche tecniche, rilevate e rischiose, rispetto alla rete e/o ai sistemi informativi aziendali – al fine di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, il personale tecnico incaricato, autorizzato dal **Responsabile dell'Ufficio Transizione Digitale**, potrà intervenire direttamente dando al Personale Esterno tempestiva comunicazione dell'avvenuto accesso.

3. Personal Computer portatili non di proprietà aziendale

L'*Azienda* ammette, in casi particolari e specificamente regolati dal rapporto contrattuale, la presenza nelle sue sedi di **Personale Esterno** dotato di Personal Computer portatili individuali non di proprietà aziendale.

Tale possibilità deve essere richiesta dal **Referente Aziendale** di riferimento tramite l'apposita funzione nell'ambito del ***Servizio di Supporto Utenti***.

Valgono le prescrizioni che seguono:

a. non è permesso l'accesso alla Rete Interna;

b. è permessa esclusivamente l'uscita in Internet e solo per fini lavorativi, ad es. per collegarsi con l'ambiente informatico della propria azienda;

c. non si possono inoltrare richieste di assistenza e/o di intervento su un PC non di proprietà aziendale;

d. il **Personale Esterno** deve svolgere solo le attività consentite ed evitare qualsiasi azione o comportamento che possa esporre all'esterno dati e/o documenti aziendali e/o informazioni soggette a *privacy*.

Qualora fossero necessarie modalità di utilizzo diverse, il **Personale Esterno** deve rivolgersi al proprio **Referente Aziendale** che, se del caso, provvede ad inoltrare specifica richiesta utilizzando l'apposita funzione nell'ambito del ***Servizio di Supporto Utenti*** e a comunicare al **Personale Esterno** le opportune istruzioni cui attenersi fornire e gli eventuali impegni da sottoscrivere.

4. Supporti rimovibili

L'*Azienda* non ammette l'utilizzo di supporti rimovibili, come ad es. chiavette USB, hard disk esterni, salvo specifica autorizzazione del **Referente Aziendale** che comunicherà le opportune istruzioni cui attenersi.

5. Credenziali di autenticazione

L'accesso al Personal Computer e alla Rete Aziendale è protetto da opportune credenziali (*userid*/*password*) consegnate al **Personale Esterno** e costituite da un codice che identifica l'utente (*userid*) associato ad una parola chiave (*password*) che consente di verificarne l'identità.

L'accesso alle Applicazioni può essere protetto da ulteriori credenziali, che possono essere identiche o diverse da quelle di accesso al Personal Computer e alla Rete Aziendale. Qualora diverse, la password viene gestita con le modalità previste dalla specifica Applicazione.

Valgono le seguenti prescrizioni:

a. al **Personale Esterno** sono assegnate le pertinenti credenziali di autenticazione il cui corretto utilizzo è obbligatorio per l'accesso all'ambiente di lavoro;

b. la password iniziale, assegnata in occasione del primo accesso, deve essere immediatamente modificata ad esclusiva cura dell'assegnatario, e successivamente deve essere obbligatoriamente modificata con la periodicità e le modalità previste dalle Procedure;

c. la composizione della password deve seguire le regole previste e non deve contenere riferimenti facilmente riconducibili all'Utente (ad es. data di nascita, nome, cognome, ecc.). I sistemi e le applicazioni sono configurati per controllare automaticamente la robustezza della password e per richiederne il cambio alla sua scadenza;

d. le credenziali (userid e password) devono essere custodite con la massima diligenza e non devono essere rivelate ad alcuno per nessun motivo;

e. non deve essere conservato nessun appunto o documento, e non deve essere inoltrato nessun messaggio (posta elettronica, cartaceo, SMS, social network, piattaforma di messaggistica, ecc.) contenente la password o riferimenti alla stessa, per evitare che altri ne vengano, anche accidentalmente, a conoscenza.

f. nel caso di sospetto che altri siano venuti a conoscenza della sua password, dovrà procedere immediatamente alla modifica della stessa e, contestualmente, segnalare l'evento come previsto nel **Capitolo 10 - Gestione degli Incidenti di Sicurezza IT**;

g. nel caso di abilitazione all'accesso da remoto alla rete aziendale tramite collegamento VPN, si devono obbligatoriamente utilizzare le credenziali di accesso ed il software allo scopo previsto, e occorre attenersi alle modalità comunicate.

In casi del tutto eccezionali l'*Azienda* si riserva la possibilità di utilizzare l'utenza personale dell'Esterno, previa forzatura delle credenziali di accesso. Tale forzatura avviene esclusivamente nei casi e con le modalità previste nella specifica Procedura che, tra l'altro, prevede l'avviso al **Personale Esterno** oltre al mantenimento della traccia delle autorizzazioni date e delle attività svolte.

6. Archiviazione dei File

Il **Personale Esterno** può essere autorizzato, in base all'attività assegnata, ad accedere e/o gestire *file* su determinate *cartelle di rete,* posizionate sui *server* dell'*Azienda*.

Valgono le seguenti prescrizioni:

a. le *cartelle di rete* 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 legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, su queste cartelle;

b. nella gestione dei *file* appoggiati su *cartelle di rete*, si devono rispettare eventuali disposizioni emanate in merito alla corretta archiviazione degli stessi, in particolare per minimizzare l'occupazione dello spazio e/o massimizzare la capacità di rintracciare contenuti utili;

c. si raccomanda la pulizia delle *cartelle di rete* – che consiste nella cancellazione dei *file* superati, inutili e duplicati – con frequenza non superiore al semestre;

d. l'archiviazione di *file* di lavoro su cartelle locali (cartelle presenti nel PC assegnato) è consentita solo per brevi periodi, pari al tempo strettamente necessario per eseguire operazioni per cui sia necessaria tale archiviazione;

e. la responsabilità del salvataggio dei file su cartelle locali è a carico del **Personale Esterno**;

f. è vietata in ogni caso l'archiviazione, nel PC assegnato, di *file* con dati personali.

Al fine di garantire la funzionalità, la sicurezza e la salvaguardia del sistema stesso o per esigenze tecniche o manutentive, personale tecnico con qualifica di Amministratore di Sistema può, in qualunque momento, procedere alla rimozione d'ufficio di elementi (*file* o cartelle) ritenuti pericolosi per la sicurezza dell'ambiente di lavoro, sia sulla rete che sul PC assegnato.

Sui *server* che ospitano le cartelle di rete vengono svolte regolari attività di controllo e di amministrazione ed in particolare sono previsti periodici salvataggi dei dati (*backup)* secondo quanto previsto dalle specifiche Procedure. Il salvataggio dei dati su copie di *backup* garantisce la possibilità di recuperare contenuti danneggiati e/o involontariamente rimossi.

7. Protezione dai virus e dai malware

Il sistema informatico aziendale è protetto da *software* antivirus mantenuto periodicamente aggiornato.

Il **Personale Esterno** comunque deve mettere in atto comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro *software* aggressivo (*malware*).

Valgono le seguenti prescrizioni:

a. è fatto assoluto divieto di disinstallare o disattivare anche solo temporaneamente l'antivirus, in quanto pericoloso per il proprio Personal Computer e per l'intera rete aziendale.

b. nel caso in cui il *software* antivirus rilevi la presenza di un virus, deve sospendere immediatamente ogni elaborazione in corso, senza spegnere il dispositivo elettronico in utilizzo, nonché segnalare prontamente l'accaduto con le modalità previste nel ***Capitolo 10 - Gestione degli Incidenti di Sicurezza IT.***

8. Navigazione Internet

Il **Personale Esterno** può essere autorizzato, in base all'attività svolta, ad accedere alla Rete Internet dal PC assegnato.

Il **Personale Esterno** deve essere consapevole che l'utilizzo improprio di questo servizio può avere conseguenze, anche rilevanti, in termini d'immagine dell'*Azienda*, di etica dell'ambiente di lavoro e di sicurezza dei sistemi informatici.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa o a rischio di sicurezza, l'*Azienda* può predisporre specifichi blocchi o filtri automatici che prevengano operazioni quali l'*upload* e/o l'accesso a determinati siti inseriti in una *black list*.

Valgono le seguenti prescrizion**i**:

a. la navigazione in Internet è riservata allo svolgimento dell'attività lavorativa e non deve essere utilizzata a fini personali.

b. non si deve effettuare l'*upload* o il *download* di software, nemmeno se gratuiti (*freeware*) o liberamente utilizzabili (*shareware*);

c. non si devono utilizzare documenti o file (filmati e/o musica) provenienti da siti web, se non strettamente attinenti all'attività lavorativa. Tale utilizzo, anche se ammesso, deve avvenire solo previa verifica dell'attendibilità dei siti in questione;

d. non si deve accedere a connessioni anonime o connessioni cifrate che non permettano l'identificazione dell'indirizzo di navigazione, o comunque a connessioni che esulano da quelle autorizzate.

Qualora, per particolari esigenze lavorative, Il **Personale Esterno** debba accedere a determinati siti inclusi nella *black list*, quest'ultimo può rivolgersi al proprio **Referente Aziendale** che, se del caso, provvederà a richiedere specifica abilitazione utilizzando l'apposita funzione nell'ambito del ***Servizio di Supporto Utenti***.

I *log* di accesso alla rete internet e i *log* di navigazione, in accordo con le disposizioni di legge vigenti, vengono mantenuti per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'*Azienda*. È in ogni caso osservato il principio di pertinenza temporale del trattamento, in modo che la tenuta dei dati sia effettivamente congrua e giustificabile alla luce delle esigenze tecniche di gestione del sistema informatico.

L'accesso ai *log* suddetti avviene esclusivamente nei casi e con le modalità previste nella specifica Procedura. Tale controllo non è continuativo, ma viene posto in essere solo nel caso che si riscontrino anomalie e viene effettuato inizialmente sulla base di informazioni anonime e aggregate, intervenendo in modo più accurato solo qualora circostanze oggettive e documentate ne giustifichino la necessità, applicando il sistema dei controlli graduali di cui al successivo ***Capitolo 11 - Sistema dei controlli.***

9. Social Media

Il **Personale Esterno** non può divulgare attraverso i Social Media contenuti o eventi dell'*Azienda* se non specificamente autorizzato dal proprio **Referente Aziendale** che comunicherà le opportune istruzioni cui attenersi.

10. Gestione degli Incidenti di Sicurezza IT

Gli **Incidenti di Sicurezza IT** si verificano sempre più frequentemente e nessuna Azienda può ritenersi immune.

Per una risposta efficace è importante una reazione rapida e per questo è necessario riconoscere tempestivamente un potenziale incidente di sicurezza IT, come ad esempio:

- la segnalazione della presenza di un possibile virus
- la rilevazione di una situazione insolita o inattesa, come ad es. una password disabilitata senza un motivo apparente
- la rilevazione di comportamenti insoliti del PC, come ad es. continui riavvii
- la violazione di dati personali (Data Breach)

Per il **Personale Esterno** valgono le seguenti prescrizioni:

a. qualora venga a conoscenza di un potenziale Incidente di Sicurezza IT deve effettuare prontamente una segnalazione seguendo la *Procedura di Incident e Problem Management,* informando il proprio **Referente Aziendale** e, in caso di particolare criticità, avvertendo immediatamente l'**Ufficio Transizione Digitale**.

11. Sistema dei controlli

L'Azienda, nel rispetto del divieto di utilizzo di strumenti tecnologici preordinati al controllo dell'attività lavorativa, assicura che strumenti tecnologici di controllo potranno essere installati, se del caso, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e/o per la tutela del patrimonio, e per tutte le finalità previste dal rapporto contrattuale e previa idonea informativa all'interessato.

Con riferimento ai sistemi informatici aziendali va tenuto presente che essi, strutturalmente – cioè per loro natura – generano, in fase di utilizzo, dei *file di log* (registrazioni) di regola aggregati o anonimi. Tali *log*, essendo tecnicamente indispensabili per il funzionamento dei sistemi informatici, fanno parte – al pari di tutti gli strumenti di lavoro elencati nel presente documento – degli strumenti necessari al personale per svolgere la propria attività lavorativa, e pertanto non necessitano di accordi o autorizzazioni.

Eventuali controlli, che in nessun caso saranno prolungati, costanti o indiscriminati, potranno avvenire secondo le seguenti indicazioni.

A. **Controllo difensivo**: in presenza di seri indizi, il personale appositamente incaricato potrà effettuare, attraverso i predetti sistemi tecnologici, controlli rivolti ad accertare condotte illecite (c.d. controllo difensivo del datore di lavoro), anche mediante verifica dei *file di log* presenti sui singoli PC, fissi o portatili, qualora con dette modalità non si pregiudichi la sicurezza del sistema e del trattamento dati.

B. **Controllo graduale**: in caso di anomalie o malfunzionamenti, il personale incaricato effettuerà, mediante l'ausilio dei sistemi installati, controlli anonimi che si concluderanno con avvisi generalizzati diretti alle persone autorizzate al trattamento dell'area o del settore in cui è stata rilevata l'anomalia, con i quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie, posteriori all'invio dell'avviso generalizzato.

C. **Controlli su base individuale**, potranno venire effettuati in via eccezionale e tassativa, oltre che nell'ipotesi sopra menzionata, anche ove ricorra una o più delle seguenti ipotesi**:**
    - quando venga presentata una specifica richiesta di informazioni da parte dell'Autorità giudiziaria;

- quando si verifichino un evento dannoso o una situazione di pericolo che richiedano un immediato e necessario intervento.

I dati raccolti dai predetti controlli potranno essere utilizzati per tutte le finalità connesse alla gestione del rapporto contrattuale, nel rispetto della normativa *privacy.*

PARTE SECONDA

12. Sanzioni

Il **Personale Esterno** è tenuto a osservare le disposizioni contenute nel presente **Regolamento Esterni**. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile secondo quanto previsto dal rapporto contrattuale e, verificata la gravità della violazione contestata, anche con la risoluzione o il recesso dal contratto, nonché con tutte le azioni civili e penali consentite.

13. Aggiornamento e revisione

Il presente **Regolamento Esterni** è soggetto a revisione periodica, almeno annuale e comunque in caso di modifiche dei processi e delle *policy* aziendali.

La versione aggiornata del Regolamento è disponibile per il personale interno sulla ***intranet aziendale*** sezione procedure interne.

A fronte di modifiche, i singoli **Referenti Aziendali** che hanno in carico il **Personale Esterno**, provvedono a raccogliere nuova sottoscrizione.

14. Entrata in vigore del Regolamento Esterni e pubblicità

Il presente **Regolamento Esterni** entra in vigore a partire dalla data di approvazione sotto riportata.

Con l'entrata in vigore tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Il presente **Regolamento Esterni** viene comunicato ai singoli soggetti interessati dai rispettivi **Referenti Aziendali** ed integra il rapporto contrattuale.

Data di approvazione del **Regolamento Esterni**: 08/07/2021

Per accettazione

Data _____ Firma_____