

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

Sommario

1. SCOPO	2
2. AMBITO OPERATIVO	2
3. FUNZIONI COINVOLTE	2
4. RIFERIMENTI NORMATIVI.....	3
5. UTILIZZO DEGLI STRUMENTI INFORMATICI	3
6. NORME GENERALI DI COMPORTAMENTO.....	4
7. GESTIONE PASSWORD.....	6
8. USO CONSAPEVOLE DI INTERNET	6
10. SALVATAGGIO E CONDIVISIONE DATI	8
11. INSTALLAZIONE DI PROGRAMMI.....	9
12. UTILIZZO DI SUPPORTI RIMOVIBILI	9
13. UTILIZZO DI STAMPANTI E FOTOCOPIATRICI	10
14. SEGRETO PROFESSIONALE	10
15. RISERVATEZZA DATI	10
16. DISCIPLINA DEROGHE E MODIFICHE DEL PRESENTE REGOLAMENTO	11

Rev.	Data	Motivo	Redatto	Verificato	Approvato
0	24.06.20	1°EMISSIONE	Gestione Amministrativa	RSGQ	Direttore Generale

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

1. SCOPO

Il presente Regolamento di funzionamento interno disciplina le modalità operative adottate dalla Fondazione Regionale per la Ricerca Biomedica (FRRB) per l'utilizzo delle risorse e della strumentazione informatica in dotazione sia allo staff che ai propri collaboratori.

2. AMBITO OPERATIVO

La Fondazione Regionale per la Ricerca Biomedica è un ente del Sistema Regionale (SIREG) costituito con Legge Regionale 30/2006 (come da ultimo modificato dall'art. 1 della L.R. 14/2010) e compreso nell'allegato A2.

FRRB, in quanto ente del SIREG, beneficia degli strumenti informatici e telematici messi a disposizione dalla Giunta di Regione Lombardia.

A tal proposito, per la gestione delle risorse e degli strumenti informatici, FRRB si avvale dei servizi messi a disposizione dalla Giunta di Regione Lombardia per il tramite una serie di soggetti da quest'ultima designati che, per le parti di propria competenza, forniscono tutto quanto necessario per il funzionamento della Fondazione (software, hardware, assistenza).

Le apparecchiature e i sistemi di infrastruttura centrale sono concessi a FRRB sulla base dell'" *Accordo per l'utilizzo degli spazi di palazzo sistema da parte della Fondazione Regionale per la Ricerca Biomedica*" stipulato con la Giunta della Regione Lombardia (Unità Organizzativa Sedi Istituzionali e Patrimonio).

Tali apparecchiature sono registrate all'interno del Registro elenco utenti, attrezzature ed apparecchiature (Allegato_11 alla P07), costantemente aggiornato dal referente informatico della Fondazione e dalla Segreteria Generale e trasmesso all'occorrenza al referente informatico di Regione Lombardia.

Il sito istituzionale e la posta elettronica, invece, sono gestiti autonomamente sulla base di singoli accordi stipulati con fornitori privati.

3. FUNZIONI COINVOLTE

Il presente documento è indirizzato a tutto il personale dipendente di FRRB, compreso il personale dirigenziale, a tutti coloro che collaborano con la Fondazione ed a tutti coloro i quali, pur in assenza di un rapporto di lavoro subordinato con l'Ente, collaborano con esso a qualunque titolo o grado, nel momento in cui usano le attrezzature informatiche dell'ente.

I soggetti sopra indicati sono tutti egualmente obbligati al rispetto degli obblighi derivanti dall'applicazione del presente Regolamento.

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

4. RIFERIMENTI NORMATIVI

- Statuto di FRRB
- Legge Regionale 27 dicembre 2006, nr. 30 che ha istituito il Sistema Regionale (SIREG) definendo i soggetti che lo costituiscono (Allegati 1 e 2)
- DGR nr. IX/2401 del 26/10/2011 con cui la Regione Lombardia (RL) ha costituito la Fondazione Regionale per la Ricerca Biomedica quale ente del Sistema degli enti regionali (SIREG) mediante il relativo inserimento negli allegati A1 e A2 della L.R. 30/2006
- Accordo per l'utilizzo di Palazzo Sistema da parte della Fondazione Regionale per la Ricerca Biomedica (rinnovato con cadenza triennale)
- Decreto nr. 13673 del 21.12.2016 di approvazione del documento "*Indirizzi per i servizi infotelematici della Giunta Regionale*" e relativo allegato
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

5. UTILIZZO DEGLI STRUMENTI INFORMATICI

Gli utenti che utilizzano gli strumenti informatici, siano essi dipendenti o collaboratori di FRRB, devono:

- a. operare in maniera responsabile a tutela della riservatezza, della protezione dei dati, dell'etica comportamentale e dell'utilizzo corretto degli strumenti informatici messi a disposizione dalla Fondazione;
- b. osservare gli obblighi posti in materia dal CCNL Commercio e dal Codice Etico di FRRB e, per i collaboratori, dal contratto di collaborazione o dal contratto di lavoro autonomo vigente;
- c. segnalare tempestivamente qualunque evento si ritenga un potenziale incidente alla sicurezza informatica (aggressioni da virus informatici, attacchi da malintenzionati interni o esterni, siti web fasulli, ecc.), al proprio Referente Informatico che provvederà a fare la segnalazione a RL, all'Help Desk contattando il numero di telefono 20000, il referente privacy e il DPO di FRRB;
- d. segnalare tempestivamente lo smarrimento o la sottrazione dell'attrezzatura assegnata al referente Informatico e all'Help Desk contattando il numero di telefono 20000, il referente privacy e il DPO di FRRB.

In quanto soggetti dipendenti o collaboratori di un ente del Sistema Regionale gli utenti degli strumenti informatici dovranno inoltre:

- a. garantire l'accesso alle risorse informatiche solo a utenti, sistemi e applicazioni autorizzati;
- b. effettuare un utilizzo responsabile del servizio fornito, in particolare per non sovraccaricare le risorse messe a disposizione;

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

- c. non eseguire in modo autonomo interventi atti a modificare la configurazione del servizio, ma far riferimento al proprio Referente Informatico che provvederà a segnalare la richiesta a RL, per avere l'autorizzazione all'intervento;
- d. fornire la propria disponibilità e supporto tecnico ad attività di verifica che RL ritenga opportune, in particolare a fronte di anomalie o incidenti, per appurare il livello di sicurezza informatica e il costante il rispetto delle politiche di sicurezza emanate;
- e. segnalare potenziali incidenti di sicurezza informatica che coinvolgano servizi forniti da RL, contattando il proprio referente informatico, che provvederà ad inoltrare la segnalazione a RL o al gestore di competenza in base alle indicazioni comunicate da RL.

6. NORME GENERALI DI COMPORTAMENTO

Tutti gli utenti ai quali è assegnata una strumentazione informatica (postazione di lavoro fissa o portatile, tablet, telefoni fissi o cellulari o altro bene informatico) devono attenersi a precise regole di comportamento di seguito elencate:

1. gli strumenti assegnati, compresi i relativi programmi l'accesso alla rete Internet, nonché le unità di rete messe a disposizione per il salvataggio dati e la condivisione di informazioni trattate in modo informatico, sono *strumenti di lavoro di RL per il tramite di FRRB* e pertanto devono essere utilizzati per motivi attinenti alla prestazione lavorativa.
E' consentito uno sporadico utilizzo anche a scopi personali, purché questo sia circoscritto nei tempi di pausa previsti dal D. Lgs. n. 66/2003 in materia di orario di lavoro; tale sporadico utilizzo non deve essere gravoso per le risorse di RL (es. sovraccarico alla rete) e non deve compromettere il funzionamento o la sicurezza dei sistemi informativi di RL, ovvero nel rispetto delle regole di comportamento indicate nei paragrafi "uso consapevole di Internet" e "uso consapevole della posta elettronica" indicate successivamente;
2. lo scambio di messaggi di posta elettronica per scopi non lavorativi deve essere effettuato da una casella personale differente da quella fornita da FRRB. A tale scopo possono essere utilizzati servizi di posta pubblicamente disponibili e accessibili via Web;
3. l'utente deve gestire le informazioni in modo lecito e secondo correttezza raccogliendole e registrandole solo per scopi inerenti all'attività svolta ovvero per le finalità previste delle mansioni assegnate e secondo i profili e le autorizzazioni concesse;
4. l'utente deve trattare in modo lecito il materiale protetto da proprietà intellettuale in qualunque sua forma (testi, immagini, audio, video, programmi, ecc.); non deve quindi fare un uso di tale materiale, (ivi incluso visione, copia, conversione, reinoltro, ecc.), anche solo di parte di esso, se non nei termini concessi dalle vigenti normative o dalle condizioni di utilizzo. L'utente deve operare garantendo la riservatezza



REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA

I016

Rev. 0
del 24.06.2020

- necessaria alle informazioni gestite in modo informatico di cui viene a conoscenza, custodendole con diligenza e non divulgandole a persone non autorizzate;
5. durante l'utilizzo dei dispositivi assicurarsi che non siano presenti persone non autorizzate e non lasciarli incustoditi, soprattutto quando l'attività lavorativa è svolta in modalità da remoto;
 6. in caso di allontanamento dalla postazione di lavoro è necessario bloccare l'accesso al proprio personal computer (sequenza di tasti CTRL + ALT + CANC e cliccare sull'opzione "Blocca Computer" o in alternativa tasto Windows + L); sulle postazioni di lavoro è inoltre configurato un salvaschermo con immissione della password;
 7. per i tablet e i telefoni cellulari, dato il forte utilizzo in mobilità e il maggiore rischio di smarrimento e furto, l'utente deve prevedere l'abilitazione di un codice di protezione del dispositivo in tutti i casi ove sia possibile;
 8. i dispositivi assegnati ai dipendenti utilizzati durante l'attività da remoto non dovranno essere esposti a rischio incendio/esplosione/allagamento o in ambienti particolarmente polverosi o in presenza di sostanze chimiche pericolose/corrosive che ne possano compromettere la funzionalità;
 9. in caso di accertato utilizzo improprio della strumentazione o di utilizzo per fini diversi da quelli consentiti per esigenze di lavoro, FRRB potrà applicare, nei confronti dell'utente, le norme disciplinari previste dal CCNL vigente;
 10. l'installazione o l'uso di programmi o componenti hardware diversi da quelli forniti è consentita solo se preventivamente autorizzata da RL. La richiesta dovrà essere effettuata da parte del referente informatico, per il tramite del Portale IT Client Management – Regione Lombardia;
 11. si richiede particolare attenzione nell'utilizzo e nella custodia dei dispositivi mobili, quali ad esempio pc portatile, tablet e telefoni cellulari, affinché non vi sia perdita o furto di informazioni gestite in modo informatico critiche o il dispositivo stesso non venga rubato. L'utente dovrà effettuare regolarmente operazioni di archiviazione (backup) delle informazioni importanti, nonché garantire la protezione delle informazioni riservate;
 12. deve essere prontamente data comunicazione al Referente Informatico e al Referente Privacy e DPO di eventuali furti, danneggiamenti o smarrimenti della strumentazione assegnata o parte di essa; inoltre l'assegnatario dovrà recarsi (personalmente e al più presto) presso un Commissariato di Pubblica Sicurezza o Stazione dei Carabinieri per sporgere regolare denuncia (completa di tutti i dati identificativi dell'utenza e/o dell'apparecchio in dotazione): copia della stessa dovrà essere fatta pervenire al proprio Referente Informatico, che provvederà a fare le opportune segnalazioni al referente di RL, nonché e al Referente Privacy e DPO affinché attivi la procedura per il Data Breach;
 13. quando uno strumento informatico non è più necessario all'assegnatario, lo stesso deve segnalarlo tempestivamente al Referente Informatico, che provvederà a

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

comunicare la riassegnazione ad altro utente o la dismissione dello strumento, previa autorizzazione di RL.

7. GESTIONE PASSWORD

La password di accesso alla postazione di lavoro e alle applicazioni è un elemento fondamentale per proteggere i dati e le informazioni da persone non autorizzate, da attacchi Internet o in caso di furto. Si evidenzia che:

- a) la password è strettamente personale e non deve essere condivisa con altri utenti;
- b) la password va cambiata al primo accesso se preimpostata, quindi periodicamente in base alle disposizioni interne fornite dal gestore del sistema informatico incaricato da RL;
- c) Il sistema chiederà all'utente di cambiare obbligatoriamente la password di accesso alla postazione di lavoro ogni 3 mesi solari.

Tutti i dipendenti e collaboratori di FRRB devono seguire le opportune procedure per la gestione della password e dell'utenza di accesso, nonché adottare un comportamento conforme alle regole di sicurezza descritte di seguito:

- a) scelta della password: la password deve essere lunga almeno 8 caratteri, oppure, nel caso in cui lo strumento non lo permetta, da un numero di caratteri pari al massimo consentito; non deve essere semplice, ovvero composta di nomi facilmente intuibili (ad esempio, evitare nomi di congiunti o parenti o qualsiasi altro insieme di caratteri alfanumerici facilmente riconducibili alla persona o all'attività svolta - date di nascita, soprannomi, ecc.); una buona password infine dovrebbe contenere lettere, maiuscole e minuscole, numeri, segni di punteggiatura e caratteri speciali;
- b) custodia della password: la password deve essere custodita in modo appropriato per mantenerne la segretezza; in particolare, non deve essere annotata e lasciata in luoghi accessibili, non deve essere comunicata a terze persone e non deve essere scritta in e-mail o allegati perché facilmente intercettabili.

E' opportuno cambiare la password ogni volta che si ha il sospetto che qualcun altro ne sia venuto a conoscenza.

8. USO CONSAPEVOLE DI INTERNET

L'utilizzo di Internet è permesso mediante la rete regionale che dispone dell'unico punto di accesso al WEB. L'utilizzo di Internet è consentito per lo svolgimento di operazioni legate all'attività lavorativa.

La rete regionale, pur essendo protetta, è comunque soggetta a rischi, i principali dei quali sono legati a:

- a) utilizzo improprio delle risorse;
- b) accesso a siti non idonei;

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

- c) possibili attacchi provenienti da codice maligno (virus, worm, cavalli di Troia e simili);
- d) mancato rispetto della legislazione sul diritto d'autore.

E' necessario che l'utente adotti comportamenti adeguati alla protezione delle risorse assegnate e delle relative informazioni trattate in modo informatico, nonostante le misure tecniche presenti, quali ad esempio antivirus, ecc. Tali comportamenti si concretizzano come segue:

- a) il nome utente e la password di accesso a Internet devono essere tenuti riservati e non possono essere condivisi con altri utenti;
- b) si fa esplicito divieto a tutti gli utenti di scaricare e installare programmi non espressamente autorizzati anche se in forma gratuita, poiché potrebbero contenere un codice malevolo;
- c) se il proprio PC è connesso alla rete interna di RL è vietato collegarlo ad un modem o ad un router (es Wi-Fi) che non siano forniti da RL;
- d) qualora si utilizzi una rete privata virtuale (Virtual Private Network – VPN), ovvero una rete protetta che tramite Internet permette di accedere da remoto direttamente alla rete di RL, deve essere applicata una particolare attenzione nell'applicazione di comportamenti descritti nel presente documento;
- e) nell'uso di reti social (ad esempio Facebook, Twitter, LinkedIn), data la caratterizzazione di tali servizi, si rimanda a quanto disciplinato nella procedura P04 par. 5.3 "Gestione di un canale social". Le pubblicazioni dovranno avere coerenza e finalità esclusivamente inerenti agli obiettivi e agli scopi della Fondazione e non potranno essere pubblicate informazioni lavorative a carattere riservato in quanto potrebbero essere viste da persone non autorizzate. Le pubblicazioni dovranno essere preventivamente autorizzate dal Direttore Generale.

9. USO CONSAPEVOLE DELLA POSTA ELETTRONICA

La posta elettronica è uno strumento fondamentale nello svolgimento dell'attività lavorativa; pertanto occorre osservare alcune precauzioni per evitare che le e-mail scambiate causino rischi ai servizi informativi di FRRB e regionali o contribuiscano a diffondere informazioni riservate trattate in modo informatico. Si ricorda inoltre che il materiale ed i contenuti inviati sono sotto diretta responsabilità dell'utente e che non è permesso inviare messaggi intimidatori, diffamatori, osceni, offensivi o comunque illeciti e/o che ledano l'immagine della Fondazione.

Vengono di seguito descritte le principali regole di comportamento:

1. la casella di posta, con i relativi messaggi, oltre che sulla postazione di lavoro è replicata su un server del gestore esterno del servizio; la gestione della casella è a carico degli utenti, che devono occuparsi di effettuare periodicamente l'archiviazione dei contenuti e la cancellazione di messaggi non più necessari;

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

2. è vietato l'invio di messaggi con sistemi a catena (per esempio messaggi che invitano a rispedire lo stesso ad altre persone) e rilanci contenenti informazioni trattate in modo informatico non riferite al mondo istituzionale;
3. l'ambiente di posta limita la dimensione massima di un messaggio e la dimensione massima degli allegati sia in invio (20 MB/E-mail) che in ricezione (20 MB/E-mail). Per tale motivo prima di allegare un documento di grosse dimensioni si consiglia di effettuarne la compressione;
4. l'ambiente di posta è capace di identificare ed eliminare i principali virus nascosti negli allegati; tuttavia è sempre possibile che qualche virus non venga intercettato. E' consigliato quindi non aprire e-mail con allegati sospetti specialmente se non se ne conosce la provenienza ed eventualmente contattare l'assistenza tecnica al numero dedicato Particolare attenzione deve essere rivolta anche a mail provenienti da indirizzi conosciuti, in quanto molti virus sono progettati per veicolarsi in rete tramite gli indirizzi contenuti nella rubrica dell'utente;
5. è vietato rispondere alla posta indesiderata (spam), o a messaggi che chiedono di effettuare operazioni che comportano inserimento di utente e password in quanto potrebbero contribuire alla diffusione e generazione di altra posta indesiderata.
6. è vietato l'invio di allegati di grosse dimensioni o a un numero elevato di persone sia interne che esterne a FRRB se non strettamente necessario. La spedizione di allegati con dimensioni eccessive o l'invio di e-mail a un numero elevato di destinatari possono compromettere il corretto funzionamento del servizio;
7. è buona norma evitare di rispondere alle e-mail rinviando allegati non necessari; prima di allegare un documento si consiglia di effettuarne la compressione e in caso di allegati che contengano più documenti, se ne consiglia la compressione in un unico file;
8. è buona norma procedere regolarmente all'archiviazione dei messaggi di posta dalla casella sul server all'unità locale o, in caso di messaggi di scarsa rilevanza o interesse, effettuarne la cancellazione; in presenza di caselle sovraccariche il sistema di posta elettronica può essere molto lento e diventare inutilizzabile;
9. è buona norma, in caso di assenze prolungate per ferie o altro, attivare un messaggio automatico che indichi il periodo di assenza ed eventualmente un altro riferimento al quale inviare i messaggi di lavoro urgenti;
10. un sistema di gestione della posta indesiderata (sistema anti-spam) filtra tutte le mail che vengono inviate dall'esterno e blocca gran parte della posta indesiderata o insicura;
11. il sistema chiederà all'utente di cambiare obbligatoriamente la password di accesso alla casella mail ogni 90 giorni.

10. SALVATAGGIO E CONDIVISIONE DATI

Le informazioni trattate in modo informatico e i documenti elaborati dagli utenti devono essere a disposizione della Fondazione; pertanto anche al fine di evitare la perdita dei file

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

causata da guasti hardware o da cancellazione involontaria è previsto un servizio di backup e ripristino dei dati da remoto.

A tal proposito FRRB dal 2018 è dotata di un sistema di archiviazione digitale – Sharepoint di Microsoft 365 -, con l'ausilio e l'assistenza di un fornitore esterno. Tale sistema permette a FRRB di avere un backup dell'intera documentazione di ciascun utente, nonché la possibilità di condivisione dei medesimi documenti tra diversi dipendenti.

Ciascun dipendente è responsabile ed ha la gestione di una propria area di competenza, protetta da una password di accesso. L'amministratore del sistema (fornitore esterno) è responsabile della gestione dei permessi e autorizzazioni che ogni singolo dipendente ha la possibilità di dare per la condivisione dei propri contenuti ad altri utenti. Trattasi di un sistema protetto da credenziali personali, che può essere consultato oltre che dal pc dato in dotazione al dipendente anche da qualsiasi altro pc tramite browser.

11. INSTALLAZIONE DI PROGRAMMI

Sul personal computer in uso non possono essere installati programmi che non siano ufficialmente forniti dal responsabile dei sistemi informativi designato da RL

FRRB ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore nr. 633/41 come novellata.

12. UTILIZZO DI SUPPORTI RIMOVIBILI

Gli utenti devono prestare la massima attenzione nell'uso dei supporti rimovibili di memorizzazione. Tale uso deve essere comunque ridotto al minimo.

In caso di utilizzo di supporti rimovibili da parte del personale, valgono le seguenti regole/linee guida:

1. evitare di utilizzare supporti di memorizzazione rimovibili (cd, dvd, memorie USB, pen drive o altri dispositivi esterni di memorizzazione come le Memory stick) la cui provenienza non è nota;
2. chi registra le informazioni trattate in modo informatico su supporti di memorizzazione rimovibili è responsabile della custodia di questi ultimi e deve operare in modo da evitare la lettura del supporto da parte di persone non autorizzate;
3. non appena viene meno la necessità di mantenere i dati su supporto rimovibile occorre provvedere alla loro cancellazione irreversibile con sovrascrittura. CD e DVD non più utilizzati devono essere distrutti a cura dell'utente;
4. Tutti i supporti di memorizzazione destinati a contenere dati riservati, se lasciati in ufficio, devono essere messi in sicurezza, a cura dell'utente, in armadi chiusi con adeguati sistemi di protezione, come ad esempio accesso mediante chiave.

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

13. UTILIZZO DI STAMPANTI E FOTOCOPIATRICI

Si raccomanda di non lasciare documenti incustoditi presso le postazioni di stampa all'atto dell'invio della copia.

Qualora il dipendente sia prossimo a fotocopiare atti contenenti dati personali o informazioni riservate, avrà cura di monitorare la postazione e preservare – limitatamente alle oggettive possibilità – la conoscibilità di tali dati o informazioni, da parte di terzi non autorizzati.

14. SEGRETO PROFESSIONALE

Il dipendente non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto da FRRB, né potrà usarle, sfruttarle o disporre in proprio o tramite terzi.

Gli obblighi del dipendente previsti in questo paragrafo non termineranno alla cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che il dipendente possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

15. RISERVATEZZA DATI

Premesso che per "*Informazioni Riservate*" si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento di mansioni per le quali il soggetto è stato assunto da FRRB:

- il dipendente si impegna a considerare le *Informazioni Riservate* come strettamente private e riservate e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni;
- il dipendente si impegna ad utilizzare le *Informazioni Riservate* unicamente allo scopo di effettuare lo svolgimento dell'attività cui è preposto e di conseguenza a non usare tali informazioni in alcun modo che arrechi danno a FRRB, né per alcun altro scopo di qualsiasi natura;
- quanto previsto dal presente paragrafo non proibisce di comunicare *Informazioni Riservate*: ad amministratori e dipendenti, anche di FRRB, avvocati, revisori, banche o altri nostri consulenti ai quali la conoscenza di tali Informazioni è necessaria al fine dell'espletamento di attività funzionali alla Fondazione stessa; a soggetti diversi da quelli specificati al precedente punto qualora ciò sia stato autorizzato da FRRB.

L'obbligo di riservatezza non opera in caso di *Informazioni Riservate*:

- che al momento in cui vengono rese note siano di pubblico dominio;
- che diventino di pubblico dominio dopo essere state rese note per causa non imputabile al dipendente;

L'impegno di riservatezza di cui al presente paragrafo si protrarrà anche dopo la cessazione

	REGOLAMENTO PER L'USO DELLE RISORSE E DELLA STRUMENTAZIONE INFORMATICA	I016
		Rev. 0 del 24.06.2020

del rapporto di lavoro e sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.

16. DISCIPLINA DEROGHE E MODIFICHE DEL PRESENTE REGOLAMENTO

Qualora FRRB intenda modificare il presente Regolamento, dovrà darne conoscenza immediata ai dipendenti tramite trasmissione, via email, della relativa revisione a cura della funzione Segreteria Generale.

Deroghe o modifiche di uno o più punti del presente Regolamento, non rendono invalidi gli altri punti.