

Versione del regolamento <b>3-0</b> Valevole dal <b>01.10.2021</b>	Classificazione di riservatezza <b>interna</b> Titolare <b>IT</b> Processi interessati <b>-</b> Lingue disponibili <b>DE, FR, IT</b>
Divisioni interessate / Settori Destinatari specifici / Distribuzione Sostituisce Attribuzione	<b>Settori centrali, Infrastruttura, M&amp;P Viaggiatori, Immobili e Società del Gruppo</b> <b>LIDI-R, A2, A20</b> <b>Versione del regolamento 2-0</b> <b>K 018.4</b>

## Gestione di strumenti di lavoro IT e dati aziendali

### Indice

<b>Elenco delle modifiche</b> .....	<b>2</b>
<b>1. Aspetti generali</b> .....	<b>3</b>
1.1 Situazione iniziale, obiettivi .....	3
1.2 Campo d'applicazione (aziende, utenti / funzione).....	3
<b>2. I miei strumenti di lavoro</b> .....	<b>3</b>
2.1 Gestione degli strumenti di lavoro IT .....	3
2.2 Password .....	3
2.3 Condizioni di utilizzo per strumenti di lavoro IT specifici .....	3
<b>3. Gestione delle informazioni</b> .....	<b>4</b>
3.1 Classificazione .....	4
3.2 Riservatezza e segretezza .....	6
3.3 Archiviazione dati e conservazione .....	6
3.4 Invio di documentazione .....	7
3.5 Supporti dati mobili .....	7
3.6 Stampa.....	7
3.7 Smaltimento .....	7
<b>4. Eventi rilevanti per la sicurezza</b> .....	<b>7</b>
<b>5. Software e app</b> .....	<b>8</b>
<b>6. Utilizzo privato, diritti della personalità e sorveglianza</b> .....	<b>8</b>
6.1 Utilizzo privato.....	8
6.2 Diritti della personalità e sorveglianza.....	8

## Elenco delle modifiche

Versione	Capitolo	Modifiche
3-0	3	Integrazione dell'istruzione K 400.16 Classificazione delle informazioni
2-0	3.1	Modifica dei requisiti di classificazione a causa della modifica della Azure Information Protection
1-0		Prima edizione

## 1. Aspetti generali

### 1.1. Situazione iniziale, obiettivi

Un'attenta gestione degli strumenti di lavoro IT e dei dati aziendali è fondamentale per la protezione dei dati personali e delle informazioni riservate, nonché per la protezione dei sistemi informatici e quindi dell'intero esercizio.

### 1.2. Campo d'applicazione (aziende, utenti / funzione)

Queste disposizioni valgono per tutte le persone che utilizzano strumenti di lavoro IT e dati aziendali di FFS SA o di FFS Cargo SA.

## 2. I miei strumenti di lavoro



I collaboratori delle FFS sono generalmente dotati di strumenti di lavoro IT per l'adempimento dei loro compiti di lavoro. A determinate condizioni, i collaboratori o i collaboratori di fornitori e partner possono anche utilizzare propri strumenti di lavoro IT, che in tal caso vengono denominati «Bring your own Device» o «BYOD» in breve.

### 2.1. Gestione degli strumenti di lavoro IT



Gestisci con cura gli strumenti di lavoro IT messi a disposizione dalle FFS e proteggili da danni e perdite.



Non lasciare incustoditi i tuoi strumenti di lavoro IT in stato di funzionamento. Quando lasci il posto di lavoro, blocca i tuoi strumenti di lavoro IT. Non prestare a terzi i tuoi strumenti di lavoro IT con i dati aziendali delle FFS.



Puoi bloccare il PC e il notebook in qualsiasi momento premendo il tasto **Windows + L** o (**Control+Alt+Canc, Invio**). Puoi bloccare anche il tablet e lo smartphone con il pulsante di spegnimento.

### 2.2. Password



**Tieni segrete le tue password personali e non condividerle con altre persone. Inserisci la tua password di nascosto dagli sguardi di terzi. Le password aziendali non possono essere utilizzate per servizi privati.**



La massima sicurezza è data da una password lunga. Pensa quindi a una sequenza casuale di parole, che puoi ricordare facilmente, creando così più difficoltà agli hacker.

Ulteriori informazioni sull'utilizzo con password FFS sono disponibili [qui](#).

### 2.3. Condizioni di utilizzo per strumenti di lavoro IT specifici



Per determinati strumenti di lavoro IT e servizi IT ci sono condizioni d'utilizzo aggiuntive. Riceverai le disposizioni corrispondenti con il dispositivo o all'attivazione del relativo servizio. Inoltre, gli strumenti di lavoro IT sono protetti da misure tecniche. Queste cosiddette «device policy» garantiscono un livello minimo di protezione (ad es. uno smartphone richiede necessariamente un codice e viene bloccato dopo un certo tempo).



### **Non ti è consentito rimuovere o eludere le misure tecniche di protezione.**

Quando accedi ai dati aziendali con dispositivi privati («BYOD») che non sono gestiti dalle FFS, devi garantire la seguente protezione minima:

- password del dispositivo di almeno 4 cifre;
- blocco automatico dopo 5 minuti;
- crittografia del dispositivo;
- iOS: cancellazione di tutti i dati (ripristino integrale delle impostazioni di fabbrica) dopo aver inserito per dieci volte la password errata del dispositivo.
- Android: cancellazione di tutti i dati nell'area di lavoro FFS dopo aver inserito per dieci volte la password errata del dispositivo.



[Qui](#) trovi tutte le informazioni necessarie per la gestione dei dispositivi mobili, in particolare per l'arrivo, il trasferimento e l'avvicendamento interno, la partenza, la sostituzione del dispositivo e l'utilizzo di un dispositivo privato («BYOD»).



Le ulteriori condizioni di utilizzo in caso di impiego di dispositivi privati («BYOD») per l'accesso a Office 365 sono disponibili [qui](#).



I «Mobile Device Services» («MDS») consentono ai collaboratori FFS di sincronizzare e-mail, voci del calendario, contatti, appunti e compiti con i dispositivi mobili approvati da FFS Informatica e di accedere alla rete aziendale FFS tramite le relative app («ICT Selfcare», «Portale dei collaboratori» ecc.).



Le condizioni di utilizzo per il servizio MDS sono disponibili [qui](#).



Tutte le informazioni sul tema Work Smart/telelavoro si trovano sulla rispettiva [pagina informativa](#).

## **3. Gestione delle informazioni**

### **3.1. Classificazione**



I dati aziendali comprendono dati e informazioni relative alle FFS. Sono inclusi i dati delle FFS e quelli di clienti, collaboratori, fornitori e partner commerciali.

I dati possono essere ad esempio sotto forma di documenti Office, e-mail, documenti cartacei, dossier del personale e fatture.

Maggiori informazioni sul tema «Classificazione delle informazioni» si trovano [qui](#).



**La/Il titolare dei dati** è responsabile dell'intero ciclo di vita dei dati ed è tenuto a realizzare la corretta predisposizione, conservazione e archiviazione. La/Il titolare dei dati garantisce che i diritti di accesso siano limitati in base alla riservatezza.

La/Il titolare dei dati, in particolare, è la persona che deposita un documento su un archivio aziendale delle FFS o apporta modifiche a un documento di questo tipo. In caso di modifiche occorre verificare la classificazione ed eventualmente adattarla.



Le FFS applicano i seguenti livelli di classificazione per i dati aziendali:

**C1 I dati pubblici** sono dati creati per il pubblico. Tra questi rientrano, ad esempio, l'orario, i dépliant di vendita o i comunicati stampa. Non è necessaria alcuna dicitura relativa alla riservatezza. Non è necessaria una nota sul documento.

**C2 I dati interni** sono dati destinati all'uso interno e ad altri destinatari selezionati. Questi includono le istruzioni interne, la rubrica telefonica o l'indirizzo di servizio. Queste informazioni sono accessibili, nell'ambito del principio di apertura, alla cerchia di destinatari con diritti di lettura:

- collaboratrici e collaboratori interni delle FFS
- persone in formazione o stagisti delle FFS
- collaboratrici e collaboratori esterni
- collaboratrici e collaboratori di società di partecipazione con una partecipazione di maggioranza delle FFS
- utenti non personali FFS

La nota «C2 – Internamente» sul documento è raccomandata, ma non obbligatoria.

**C3 I dati confidenziali** sono dati particolarmente sensibili. Questi includono i rapporti finanziari, la documentazione relativa a tecnologie critiche, i protocolli delle riunioni di CdA, Direzione del Gruppo e direzione della Divisione e i dati personali particolarmente sensibili.

**Sui documenti confidenziali si deve apporre obbligatoriamente la nota**

**«C3 – Confidenziale» e limitare l'accesso alla cerchia di destinatari necessari.**

L'utilizzo di dati confidenziali per scopi personali, commerciali o pubblici o l'utilizzo per studio o ricerca è consentito esclusivamente previa autorizzazione scritta delle FFS (di norma da parte del titolare dei dati in accordo con il singolo Servizio giuridico).

Le informazioni soggette a un particolare obbligo di segretezza (ad es. documenti del servizio informativo) sono considerate come «confidenziali personali». Il relativo coordinamento documenti è soggetto a disposizioni particolari e i collaboratori sono vincolati agli obblighi di segretezza corrispondenti.



Le applicazioni Office semplificano la classificazione dei documenti e contribuiscono a proteggere le informazioni riservate con più efficacia. Basta premere un tasto per classificare il documento e applicare la nota in modo automatico sul documento.



Per i documenti e le e-mail «confidenziali personali» si raccomanda il livello più elevato «C3.3 – Cifrato personale». In questo modo l'accesso può essere ridotto a una cerchia di destinatari molto limitata, indipendentemente dal

luogo di archivio, grazie alla crittografia.

C3.3 è anche la classificazione corretta in caso di scambio di e-mail e documenti riservati con uffici esterni che non dispongono di account FFS.

In casi eccezionali, ad es. se si verificano problemi tecnici nella collaborazione, è possibile utilizzare provvisoriamente, con la dovuta cautela, il livello «C3.1 – Non cifrato».

### 3.2. Riservatezza e segretezza



**Tratta i dati aziendali delle FFS con la necessaria cautela.** Anche i dati interni non devono diventare di dominio pubblico. Tuttavia, all'interno delle FFS ci scambiamo apertamente i dati classificati come «interni» e li usiamo per una collaborazione intersettoriale, a favore delle FFS (il cosiddetto «principio di apertura»).



L'utilizzo attento dei dati aziendali è un elemento fondamentale del [Codice di condotta delle FFS](#).



**Proteggi le conversazioni aziendali riservate, i contenuti aziendali di colloqui, i documenti cartacei e i supporti dati mobili, così come i contenuti sul tuo schermo e tienili al sicuro da accessi non autorizzati.**



Nell'[ICT Service Portal è disponibile un filtro privacy per lo schermo del tuo notebook](#). Seleziona il portale ordinazioni, inserisci il criterio di ricerca «filtro privacy» e otterrai una selezione di filtri privacy per lo schermo di vari tipi di notebook.

Se possibile, utilizza una sala concentrazione con chiusura a chiave per le conversazioni riservate. Il compartimento di un treno e/o i ristoranti non sono luoghi adatti a conversazioni telefoniche riservate.

Non lasciare documenti cartacei e supporti dati mobili accessibili in giro e prenditene cura, soprattutto al di fuori degli spazi di lavoro.

### 3.3. Archiviazione dati e conservazione



**Salva i dati aziendali sui servizi messi a disposizione dalle FFS (SharePoint, OneDrive for Business, DMS, filer ecc.).** I servizi cloud privati (Dropbox o iCloud privati) non sono consentiti per il salvataggio dei dati aziendali. I dati con livello di classificazione «confidenziale» vanno depositati in un archivio con diritti di accesso opportunamente limitati.



I documenti fisici con classificazione «C2 – Internamente» vanno conservati in un'area protetta (zona di protezione 1 o superiore).

I documenti fisici con classificazione «C3 – Confidenziale» vanno conservati al chiuso in un'area protetta (zona di protezione 1 o superiore).



Puoi trovare informazioni sul salvataggio dei dati in SharePoint, OneDrive for Business e DMS sulla [pagina dell'ICT Workplace](#).



Trovi informazioni sul sistema delle zone di protezione nel [Manuale Security delle FFS](#) e nel [relativo sistema delle zone di protezione](#).

### 3.4. Invio di documentazione



**Per lo scambio aziendale di messaggi (e-mail o messaggi istantanei) utilizzare i sistemi ufficiali FFS del workplace IT. Non inoltrare messaggi aziendali a servizi e-mail o di messaggistica privati.** L'invio fisico non è raccomandato, ma, se necessario, deve avvenire esclusivamente in busta chiusa.



**Trasmetti sempre le informazioni riservate in modo crittografato. Queste non possono essere trasmesse a soggetti terzi esterni senza il consenso del o della titolare dei dati.**



Ulteriori disposizioni sull'utilizzo della comunicazione elettronica e dei social media sono disponibili qui: [Principi di comportamento della comunicazione elettronica](#) e [Social Media Guide](#)

### 3.5. Supporti dati mobili



I supporti dati mobili devono essere utilizzati solo per i dati pubblici (ad es. video aziendali di grandi dimensioni che superano la capacità di memoria). I dati aziendali con la classificazione «internamente» o «confidenziale» devono essere salvati negli appositi spazi di salvataggio aziendali (ad es. SharePoint o OneDrive for Business). Per lo scambio di dati è necessario utilizzare la funzione di autorizzazione.



Tramite SharePoint è possibile condividere i dati aziendali non solo internamente alle FFS, ma anche con terzi. Puoi scoprire come fare in questa istruzione sulla [pagina dell'ICT Workplace](#).

### 3.6. Stampa



I documenti confidenziali devono essere stampati solo con la funzione «Stampa confidenziale» o mediante «FollowMe Printing».

### 3.7. Smaltimento



I documenti e i supporti di memorizzazione fisici vanno smaltiti correttamente negli appositi contenitori.



Inoltre ci si deve assicurare che il software venga tenuto aggiornato e che vengano subito installati gli update di sicurezza disponibili.

## 4. Eventi rilevanti per la sicurezza



Segnala immediatamente la perdita o il furto di dispositivi con dati aziendali, incidenti rilevanti nell'area della sicurezza delle informazioni ed eventuali violazioni della protezione dei dati all'ICT Service Desk (telefono **+41 51 220 30 40**).

## 5. Software e app



Per scopi aziendali, utilizza sempre il software acquistato e concesso in licenza dalle FFS.

Se utilizzi un software non fornito dalle FFS per scopi aziendali (sia sui dispositivi delle FFS che sui dispositivi BYOD), sei responsabile di garantire che il software possa essere utilizzato anche per scopi aziendali e che sia correttamente concesso in licenza.



Ulteriori prodotti software possono essere ordinati tramite l'[ICT Service Portal](#).

## 6. Utilizzo privato, diritti della personalità e sorveglianza

### 6.1. Utilizzo privato



Gli strumenti ICT messi a disposizione dalle FFS sono destinati principalmente all'utilizzo aziendale. I collaboratori possono utilizzarli anche per scopi privati in misura ed entro limiti ragionevoli.



**Non aprire siti web con contenuti illegali o offensivi (sessisti, razzisti, estremisti, pornografici, immorali, diffamatori).** Se hai aperto per errore una pagina di questo tipo, richiudila immediatamente.



L'accesso può essere limitato o vietato tramite istruzioni di lavoro nell'ambito della proporzionalità, ad esempio se la persona è incaricata di funzioni di sorveglianza.

Il tuo diretto superiore può limitare o vietare l'uso di Internet nell'ambito della proporzionalità se vi è il sospetto fondato o la certezza che l'uso privato superi la misura consentita o se vengono visitate pagine illegali o offensive.



**Non sono consentiti acquisti di servizi con gli abbonamenti mobili, ad es. tramite fattura del cellulare, SMS a pagamento o pagamenti tramite SMS per scopi privati.**



Informazioni dettagliate sul pagamento tramite smartphone (con un abbonamento mobile delle FFS) sono disponibili nel contributo: [Effettuare pagamenti con lo smartphone FFS](#).

### 6.2. Diritti della personalità e sorveglianza



Per garantire il funzionamento, è in parte necessaria la sorveglianza degli strumenti di lavoro IT delle FFS.

Con adeguate misure di sorveglianza e valutazione si garantisce il rispetto di tutte le disposizioni di legge e delle norme interne, così come degli accordi con le parti sociali. Si assicura inoltre che le misure rappresentino la minima violazione possibile dei diritti della personalità.

Nelle misure di sorveglianza, le FFS tengono conto del principio di proporzionalità e utilizzano esclusivamente quelle misure di valutazione e



sorveglianza che, per lo scopo prefissato, rappresentano una violazione minima dei diritti della personalità.



Trovi maggiori informazioni nella [Istruzione K 155.1](#).

IT

IT

sig. Marcus Griesser  
CISO

sig. Daniel Wild  
Security and Risk Manager