



Versione del regolamento	3-0	Classificazione di riservatezza	interno
Valevole dal	1.1.2013	Titolare	IT-SR
Ultima revisione		Processi interessati	Gestione informatica
Prossima revisione		Lingue disponibili	DE, FR, IT
Divisioni interessate		Infrastruttura, Viaggiatori, Cargo, Immobili, Gruppo	
Destinatari specifici / Distribuzione			
Sostituisce		Versione del regolamento dell'1.1.2012	

Istruzione del Gruppo sull'uso consentito di hardware e software informatici

1.	Aspetti generali	3
1.1.	Premesse, obiettivi	3
1.2.	Ambito di validità	3
1.3.	Documenti di riferimento e correlati	3
2.	Misure di sicurezza amministrative	3
3.	Disposizioni relative all'hardware	3
3.1.	Principi relativi all'uso dell'hardware	3
3.1.1.	Uso consentito dell'hardware	3
3.1.2.	Prestito prolungato gratuito di hardware	4
3.1.3.	Utilizzo per scopi privati del PC, del laptop o di mezzi ausiliari informatici messi a disposizione	4
3.1.4.	Utilizzo di PC o laptop privati per scopi di lavoro	4
3.1.5.	Blocco della postazione di lavoro	4
3.2.	Supporti	4
3.3.	Disposizioni sugli apparecchi IT portatili sui quali vengono elaborati dati delle FFS	5
3.3.1.	Disposizioni relative agli apparecchi IT portatili messi temporaneamente a disposizione	5
3.3.1.1.	Consegna o restituzione di apparecchi IT portatili messi a disposizione	5
3.3.1.2.	Protezione dal furto per gli apparecchi IT portatili	5
3.3.1.3.	Trasporto	5
3.3.1.4.	Smarrimento	5
3.4.	Salvataggio dei dati, cestino, cartelle temporanee, salvataggio automatico	5
3.5.	Modifiche	5
4.	Disposizioni relative al software e ai dati	6
4.1.	Utilizzo	6
4.2.	Test dei meccanismi di protezione delle interfacce browser per le applicazioni	6
4.3.	Uscita di un lavoratore dall'azienda	7
4.4.	Cancellazione di dati di lavoratori con disdetta senza preavviso, deceduti, scomparsi o esonerati	8
4.5.	Elaborazione di dati classificati e di dati personali	8
4.6.	Protocollo d'utilizzo	8

4.7. Controlli.....8

4.8. Modifiche8

5. Rapporto con altre istruzioni8

6. Entrata in vigore.....9

Elenco delle modifiche.....9

1. Aspetti generali

1.1. Premesse, obiettivi

La presente istruzione disciplina il tipo di utilizzo consentito di hardware e software informatici.

1.2. Ambito di validità

È valida per tutte le persone fisiche che utilizzano hardware e/o software informatici messi a disposizione dalle FFS, dai relativi partner di outsourcing (provider) o da FFS Cargo.

Tutte le persone fisiche soggette alle disposizioni della presente istruzione sono di seguito denominate «utenti» e la forma maschile include generalmente anche le rappresentanti del genere femminile a scopo di una migliore leggibilità.

1.3. Documenti di riferimento e correlati

K 30.1 Manuale Security FFS

2. Misure di sicurezza amministrative

Il diretto superiore fa in modo che gli utenti suoi sottoposti siano informati sull'esistenza e sulle disposizioni centrali della presente istruzione [compresa la relativa «Direttiva sull'utilizzo consentito di Internet, dei programmi e dei servizi di posta elettronica e sull'uso di hardware e software informatici» (K 400.5 di seguito denominata «direttiva»)]. Il superiore fa presente che l'istruzione, unitamente alla relativa direttiva, può essere visionata e scaricata in qualsiasi momento dall'Intranet delle FFS, nella rubrica Regolamenti FFS.

3. Disposizioni relative all'hardware

3.1. Principi relativi all'uso dell'hardware

3.1.1. Uso consentito dell'hardware

Presso le FFS e FFS Cargo è consentito utilizzare solo hardware acquistato e messo a disposizione dell'utente dalle FFS (o dai relativi partner di outsourcing) o da FFS Cargo per lo svolgimento delle sue funzioni.

Con provvedimenti tecnici od organizzativi, le FFS e FFS Cargo hanno facoltà di appurare la presenza di hardware utilizzato senza autorizzazione presso le FFS o FFS Cargo e di toglierlo dalla circolazione.

L'hardware deve essere trattato con cura.

3.1.2. Prestito prolungato gratuito di hardware

Per ogni prestito gratuito superiore ai due mesi di hardware, messo a disposizione delle FFS o di FFS Cargo da partner di outsourcing delle FFS e destinato ad essere usato al di fuori dei locali delle FFS o di FFS Cargo, è necessaria l'autorizzazione preliminare del capo della divisione di competenza e, qualora fosse accordata, si deve stipulare con il terzo un contratto scritto di comodato e informare immediatamente FFS IT Account Management in merito all'hardware preso a prestito (l'informazione deve indicare quale hardware è stato prestato a chi e per quanto tempo).

3.1.3. Utilizzo per scopi privati del PC, del laptop o di mezzi ausiliari informatici messi a disposizione

Non è consentito utilizzare per scopi privati durante il tempo di lavoro il PC, il laptop o i mezzi ausiliari informatici (scanner, masterizzatori, ecc.) messi a disposizione. Sono fatti salvi i casi in cui il diretto superiore ha dato la propria autorizzazione per un breve periodo.

L'utilizzo per scopi privati del PC, del laptop o dei mezzi ausiliari informatici messi a disposizione al di fuori del tempo di lavoro è ammesso in un ambito temporale limitato, a condizione che il diretto superiore non lo abbia proibito.

3.1.4. Utilizzo di PC o laptop privati per scopi di lavoro

È consentito collegare PC/laptop privati alla rete di comunicazione dati delle FFS solo previa approvazione scritta di Operation Management e di ICT-Security & Risk Management (di seguito IT-SR) dopo una omologazione in conformità a K 400.30. Sono fatti salvi i casi in cui è stato approvato un accesso remoto e se l'accesso alla rete non avviene dai locali delle FFS o di FFS Cargo.

3.1.5. Blocco della postazione di lavoro

Il PC e il laptop devono essere bloccati automaticamente al più tardi al momento di lasciare il posto di lavoro (ad esempio con un salvaschermo protetto da password), in modo da impedire qualsiasi accesso a persone non autorizzate.

In caso di inutilizzo prolungato del PC/laptop e di fine del lavoro, l'utente deve scollegarsi (logout) e spegnere il PC/laptop.

3.2. Supporti

I supporti (dischetti, CD-ROM, dischi fissi, nastri magnetici, stampe) non devono essere lasciati in giro consentendo a persone non autorizzate di copiarli, visionarli o sottrarli.

3.3. Disposizioni sugli apparecchi IT portatili sui quali vengono elaborati dati delle FFS

3.3.1. Disposizioni relative agli apparecchi IT portatili messi temporaneamente a disposizione.

3.3.1.1. Consegna o restituzione di apparecchi IT portatili messi a disposizione

Le unità organizzative delle FFS e di FFS Cargo, che prestano apparecchi IT portatili, fanno in modo che venga attuato un adeguato controllo sugli apparecchi presi in prestito.

L'utente dell'apparecchio IT portatile messo a disposizione deve cancellare i dati che ha salvato sul disco fisso prima di restituire l'apparecchio IT portatile. Gli eventuali dati ancora presenti, relativi all'utilizzo personale, devono essere cancellati dall'Help Desk (Service Desk) o dal supporto utenti dopo la restituzione dell'apparecchio IT portatile.

3.3.1.2. Protezione dal furto per gli apparecchi IT portatili

L'utente di un apparecchio IT portatile è tenuto a fare il possibile per proteggere da un possibile furto l'apparecchio IT portatile messogli a disposizione.

3.3.1.3. Trasporto

È consentito trasportare gli apparecchi IT portatili solo se ben imballati.

3.3.1.4. Smarrimento

In caso di smarrimento o furto di un apparecchio IT portatile messo a disposizione dalle FFS, dal suo partner di outsourcing o da FFS Cargo, in ragione della possibile perdita di dati è necessario comunicare lo smarrimento o il furto immediatamente anche al settore IT-SR, in modo che possano essere prese le misure di protezione possibili e necessarie (ad esempio blocco dell'account ecc.).

3.4. Salvataggio dei dati, cestino, cartelle temporanee, salvataggio automatico

IT-SR ha facoltà di emanare regolamentazioni relative al salvataggio e all'archiviazione dei dati, alle cartelle temporanee, al salvataggio automatico e alle procedure antivirus nella direttiva relativa alla presente istruzione.

3.5. Modifiche

Le modifiche all'hardware messo a disposizione (compresi i mezzi ausiliari informatici messi a disposizione) possono essere eseguite esclusivamente dal servizio di assistenza informatica. Sono fatte salve le concessioni eccezionali del settore IT-SR, che è tuttavia tenuto a fornire orientamenti al CISO sulle deroghe accordate.

4. Disposizioni relative al software e ai dati

4.1. Utilizzo

Sui computer/laptop delle FFS o di FFS Cargo è consentito utilizzare esclusivamente software autorizzato dalle FFS o da FFS Cargo. L'elenco dei software autorizzati è disponibile presso l'ufficio di gestione centrale delle licenze di FFS IT, oppure può essere consultato nel rispettivo carrello (ad esempio carrello IT WORKPLACE). Disposizioni integrative relative al software possono risultare dalla direttiva relativa alla presente istruzione.

4.2. Test dei meccanismi di protezione delle interfacce browser per le applicazioni

Le applicazioni che si possono richiamare con un browser web devono essere protette in via preventiva da possibili attacchi. Prima della messa in produzione, l'interfaccia browser di tali applicazioni va testata per verificarne la capacità di resistenza.

Ciò riguarda tutte le applicazioni utilizzabili con un browser web e presenti nella rete FFS.

Inoltre riguarda le applicazioni trasferite su sistemi di altri operatori. Tali applicazioni devono essere protette dagli attacchi in fase di sviluppo secondo criteri di best practice.

Prima della messa in produzione i meccanismi di protezione di tali applicazione vanno testati contro gli attacchi.

Le applicazioni produttive devono essere testate al momento dello sviluppo di nuove versioni, qualora vengano apportate modifiche che riguardano il rispettivo accesso tramite browser web, ma come minimo ogni due anni.

4.2.1 Sviluppi propri di FFS Informatica

Testfactory FFS viene incaricata di preparare, eseguire e valutare i test dei meccanismi di protezione delle interfacce browser.

La messa in produzione dell'applicazione o di una nuova versione può avvenire solo dopo la presentazione di una conferma della divisione operativa Security FFS.

4.2.2 Applicazioni sviluppate e gestite da altri operatori

Gli altri operatori che sviluppano e gestiscono tali applicazioni per le FFS devono essere tenuti a dimostrare che

hanno analizzato e valutato i meccanismi di protezione contro gli attacchi attraverso l'interfaccia browser web. In alternativa possono anche affidare a Testfactory FFS l'incarico di testare le applicazioni.

Il coordinamento delle dimostrazioni compete a Testfactory FFS.

4.2.3 Report

Testfactory FFS mette periodicamente a disposizione di IT Security un reporting sui test delle applicazioni.

4.2.4 Disposizioni transitorie

Le applicazioni già produttive il 1° gennaio 2012 devono essere testate a posteriori in merito ai meccanismi di protezione.

Testfactory pianifica questa verifica con i responsabili preposti alle applicazioni in base alle priorità seguenti:

1. le applicazioni raggiungibili dall'esterno tramite browser web, da Internet o dalla rete business, devono essere testate entro il 31.12.2012;
2. le applicazioni Intranet che elaborano dati confidenziali e
3. tutte le restanti applicazioni Intranet che elaborano dati interni devono essere testate entro il 31.12.2013.

4.3. Uscita di un lavoratore dall'azienda

Ogni lavoratore in uscita dalle FFS o da FFS Cargo è tenuto, quattro settimane prima della propria uscita, in accordo con il proprio superiore, a definire la sede di archiviazione per l'acquisizione di dati e/o mail salvati localmente e che saranno riutilizzati. Cancellare i dati puramente privati o non più necessari.

4.4. Cancellazione di dati di lavoratori con disdetta senza preavviso, deceduti, scomparsi o esonerati

I servizi del Personale (Human Resources) delle FFS e di FFS Cargo precisano ai familiari dei lavoratori deceduti/scomparsi e ai lavoratori esonerati o che hanno ricevuto disdetta senza preavviso, che potranno presentare alle FFS o a FFS Cargo una domanda di restituzione dei dati puramente privati entro un mese da quando il lavoratore non è più stato presente sul posto di lavoro. Essi devono comunicare per tempo al servizio di assistenza informatica nomi e cognomi dei lavoratori esonerati, deceduti, scomparsi o che hanno ricevuto disdetta senza preavviso nonché l'inizio del termine di un mese.

4.5. Elaborazione di dati classificati e di dati personali

Se su un apparecchio IT vengono elaborati dati segreti o riservati o dati personali, occorre adottare particolari provvedimenti tecnici per proteggerli da un possibile accesso da parte di persone non autorizzate. Il servizio di assistenza informatica offre consulenza e supporto agli utenti su questo argomento.

4.6. Protocollo d'utilizzo

Nell'ambito di quanto consentito dalla legge ed esclusivamente per ragioni di sicurezza tecnica IT (in particolare non per controllare i lavoratori), l'unità organizzativa IT-SR può eseguire controlli anonimi a campione sugli accessi a programmi e file in base a orari definiti e per una durata limitata. I dati vengono memorizzati esclusivamente in forma resa anonima e cancellati immediatamente dopo l'uso.

4.7. Controlli

IT-SR ha facoltà di analizzare schematicamente a mezzo computer i contenuti che passano per il sistema IT e le reti delle FFS che indicano la presenza di rischi quali virus, worm, sovraccarichi del sistema, ecc. Questi processi sono completamente automatici in base alle possibilità tecniche correnti. I dati vengono memorizzati in forma resa anonima e cancellati immediatamente dopo l'uso.

4.8. Modifiche

Le modifiche al software messo a disposizione possono essere eseguite esclusivamente dal servizio di assistenza informatica. Sono fatte salve le concessioni eccezionali del CISO o del CIO. Quest'ultimo deve fornire orientamenti al CISO sulle deroghe accordate.

5. Rapporto con altre istruzioni

Nell'ambito della competenza ad esso delegata con la presente istruzione (cfr. ad esempio il punto 4.1 della presente istruzione), IT-SR ha facoltà di emanare disposizioni esecutive relative all'utilizzo consentito di hardware e software informatici nella «Direttiva sull'utilizzo consentito di Internet, dei programmi e dei servizi di posta elettronica e sull'uso di hardware e software informatici». Tuttavia, le disposizioni di detta direttiva non devono essere in contrasto con le disposizioni della presente istruzione.

Le modifiche apportate da IT-SR alla direttiva e che risultano da una norma di delegazione della presente istruzione devono essere sottoposte a un controllo giuridico preliminare.

6. Entrata in vigore

La presente istruzione entra in vigore il 1.1.2013.

IT

IT-SR

F.to Peter Kummer
CIO

F.to Marcus Griesser
CISO

Elenco delle modifiche

Versione	Valevole dal	Capitolo	Modifica
3-0	1.1.2013	Tutti	Acquisizione dell'istruzione nel modello attuale del regolamento e aggiornamento formale delle definizioni delle funzioni. Passaggio da K-IT a IT.