

Versione del regolamento	<b>2-0</b>	Classificazione di riservatezza	<b>interno</b>
Valevole dal	<b>1.1.2013</b>	Titolare	<b>IT-SR</b>
Ultima revisione		Processi interessati	<b>Gestione informatica</b>
Prossima revisione		Lingue disponibili	<b>DE, FR, IT</b>
Divisioni interessate	<b>Infrastruttura, Viaggiatori, Cargo, Immobili, Gruppo</b>		
Destinatari specifici / Distribuzione			
Sostituisce	Versione del regolamento del 1.5.2010		

## Direttiva sull'utilizzo consentito di Internet, dei servizi e programmi di posta elettronica e sull'uso di hardware e software informatici

<b>1. Aspetti generali</b>	<b>3</b>
1.1 Premesse, obiettivi	3
1.2 Ambito di validità	3
1.2 Documenti di riferimento e correlati	3
1.3 Termini e abbreviazioni	3
<b>2. Disposizioni relative al software</b>	<b>4</b>
2.1 Utilizzo di software privato su PC/laptop (punto 4.1, K 400.9)	4
2.2 Installazione/disinstallazione di software (punto 4.1, K 400.9)	4
2.3 Software messo a disposizione (punto 4.1, K 400.9)	4
2.4 Esigenza di un software nuovo o diverso (punto 4.1 K 400.9)	4
2.5 Modifica delle impostazioni di configurazione (punto 4.1, K 400.9)	5
2.6 Copia e conferimento di diritti d'uso per il software (punto 4.1, K 400.9)	5
2.7 Principi relativi all'utilizzo delle password (punto 4.1, K 400.9)	5
2.8 Principi relativi all'utilizzo degli account di amministratore	6
<b>3 Disposizioni relative all'hardware</b>	<b>6</b>
3.1 Campo di regolamentazione	6
3.2 Collocazione (punto 3 K 400.9)	6
3.3 Collegamenti in rete (punto 3 K 400.9)	6
3.4 Modem (punto 3 K 400.9)	7
3.5 Accesso remoto via IPSec VPN da PC/laptop privati (punto 4.4 K 400.9)	7
3.6 Salvataggio e archiviazione dei dati (punto 3.4 e 4.1 K 400.9)	7
3.7 Protezione antivirus (punti 3.4 e 4.1 K 400.9)	8
3.8 Protezione antivirus per collegamenti di accesso remoto (punti 3.4 e 4.1, K 400.9)	8
3.9 Comunicazione tramite reti pubbliche wireless (Public GSM, Public WLAN) (punti 3 e 4.1 K 400.9)	9
3.10 Collegamento a reti non soggette al controllo delle FFS (p. es. Internet, WLAN private) (punti 3 e 4 K 400.9)	9
3.11 Smarrimento e furto (punti 3 e 4.1 K 400.9)	9
3.12 Comunicazione di eventi e rischi rilevanti per la sicurezza (punti 3 e 4.1 K 400.9)	9
<b>4 Utilizzo consentito di Internet</b>	<b>9</b>
4.1 Utilizzi rischiosi (punto 3.1.3 K 400.8)	9
4.2 Divulgazione di dati sensibili (punto 3.1.3 K 400.8)	10

<b>5</b>	<b>Utilizzo consentito di servizi e programmi di posta elettronica.....</b>	<b>10</b>
5.1	Informazione e supporto (punto 4.4 K 400.8) .....	10
5.2	Utilizzo di sistemi di posta elettronica (client) (punto 4.4 K 400.8) .....	10
5.3	Comunicazione prudente dell'indirizzo di posta elettronica in caso di pericolo di spam (punto 4.4 K 400.8) .....	10
5.4	Messaggi di posta elettronica privati (punto 4.4 K 400.8) .....	11
5.5	Allegati/Attachment (punto 4.4 K 400.8) .....	11
5.6	Invio di messaggi di posta elettronica (punto 4.4 K 400.8) .....	11
5.7	Riservatezza/ Codifica (punto 4.4 K 400.8) .....	11
5.8	Firma digitale (punto 4.4 K 400.8) .....	12
5.9	Ricezione di messaggi di posta elettronica (punto 4.4 K 400.8) .....	12
5.10	Posta elettronica e stipulazione di contratti (punto 4.4 K 400.8) .....	12
5.11	Allegati ai messaggi di posta elettronica (punto 4.4 Z 400.8 e punto 5.1 K 400.8) .....	12
5.12	Programmi ricevuti mediante posta elettronica (punto 4.4 K 400.8) .....	12
5.13	Hoax ricevuti tramite posta elettronica (punto 4.4 K 400.8) .....	13
5.14	Regolamento per il sostituto (punto 4.4 K 400.8) .....	13
5.15	Salvataggio/Archiviazione (punto 4.4 K 400.8) .....	13
5.16	Controllo (punto 4.4 K 400.8) .....	13
6.	Entrata in vigore .....	14
	<b>Elenco delle modifiche.....</b>	<b>14</b>

## 1. Aspetti generali

### 1.1 Premesse, obiettivi

La presente direttiva disciplina le fattispecie, che ICT Security & Risk Management è autorizzato a regolamentare sulla base di una norma di delegazione espressamente prevista dalle istruzioni del Gruppo sull'utilizzo consentito di Internet e dei servizi e programmi di posta elettronica (K 400.8), nonché sull'uso consentito di hardware e software informatici (K 400.9).

### 1.2 Ambito di validità

È valida per tutte le persone fisiche che utilizzano hardware e/o software informatici, internet, servizi e programmi di posta elettronica per mezzo di un accesso locale o remoto, messi a disposizione da FFS SA, dai relativi partner di outsourcing (provider) o da FFS Cargo SA.

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.

### 1.2 Documenti di riferimento e correlati

K 400.8 «Istruzione del Gruppo sull'utilizzo consentito di Internet e dei servizi e dei programmi di posta elettronica»

K 400.9 «Istruzione del Gruppo sull'uso consentito di hardware e software informatici»

### 1.3 Termini e abbreviazioni

All'interno della presente direttiva si utilizzano i seguenti concetti:

Concetto	Descrizione
Account	Conto dell'utente
Attachment	File allegato a un messaggio e-mail
Utente	Utilizzatore di hardware e/o software, di Internet e/o di servizi e/o programmi di posta elettronica
CISO	Chief Information Security Officer delle FFS
NSM	Network Security Manager
Folder	Cartella che contiene file
Palmare	Piccolo computer (Psion, Communicator o simili)
Hardware	Insieme degli apparecchi e dei componenti tecnici di un impianto per l'elaborazione di dati
Hash	Checksum risultante da un algoritmo di codifica che garantisce l'integrità di un documento.
Hoax	E-Mail con informazioni errate (quasi sempre avvisi di virus), spesso con richiesta di inoltrare.
IT	Tecnologia dell'informazione. Apparecchi elettronici per l'elaborazione, la registrazione, il salvataggio e il backup di dati.
JavaScript/ActiveX	Applicazioni per la visualizzazione di elementi speciali di Internet.
Login/Logout	Messaggio di inizio e fine sessione all'attenzione del sistema IT.
Istruzione sull'utilizzo di Internet	Corrisponde all'istruzione del Gruppo sull'utilizzo consentito di Internet e dei servizi e programmi di posta elettronica (R Z 400.8).
Istruzione sull'uso di hardware e software	Corrisponde all'istruzione del Gruppo sull'uso consentito di hardware e software informatici (R Z 400.9).

Software	Concetto collettivo per i programmi eseguiti su un computer.
CISO	Chief Information Security Officer

## 2. Disposizioni relative al software

### 2.1 Utilizzo di software privato su PC/laptop (punto 4.1, K 400.9)

È vietato utilizzare software privato sui PC/laptop messi a disposizione dalle FFS, dal relativo partner di outsourcing (cfr. punto 1, cpv. 1 Z 400.9) o da FFS Cargo. Le eccezioni possono essere autorizzate dal superiore – dopo avere richiesto il consenso del servizio di assistenza informatica e del CISO delle FFS.

### 2.2 Installazione/disinstallazione di software (punto 4.1, K 400.9)

Il software può essere installato e disinstallato soltanto dai servizi di assistenza informatica.

È vietata l'installazione di software non acquisito dalle FFS o da FFS Cargo.

### 2.3 Software messo a disposizione (punto 4.1, K 400.9)

Il software eventualmente messo a disposizione dalle FFS o da FFS Cargo per PC o laptop privati può essere impiegato solo agli scopi previsti dalle FFS o da FFS Cargo. Una volta concluso il rapporto di lavoro o di incarico con le FFS o FFS Cargo, tale software deve essere cancellato dal PC o dal laptop privato e non può più essere utilizzato.

### 2.4 Esigenza di un software nuovo o diverso (punto 4.1 K 400.9)

Se occorre un software nuovo o diverso, si deve contattare il servizio di assistenza informatica dopo avere consultato il proprio superiore.

**2.5 Modifica delle impostazioni di configurazione (punto 4.1, K 400.9)**

L'utente non può modificare le impostazioni di configurazione del software (p.es. il livello di sicurezza del browser o le impostazioni di controllo del programma antivirus). Se si desidera una determinata impostazione di configurazione, si deve presentare un'apposita richiesta del superiore al rispettivo responsabile software - al CISO nel caso di impostazioni di sicurezza.

**2.6 Copia e conferimento di diritti d'uso per il software (punto 4.1, K 400.9)**

È vietato copiare il software. Restano riservati i casi in cui questa operazione è chiaramente consentita a livello legale (p.es. a scopi di sicurezza) ed è stata precedentemente autorizzata dal responsabile del Centro soluzioni competente.

È vietato concedere a persone fisiche o giuridiche diritti d'uso o sublicenze di software per cui le FFS o FFS Cargo non dispongano del diritto d'autore, né siano autorizzate (soprattutto da contratto) ad effettuare tale conferimento. In caso di dubbio, si deve prima chiedere al servizio giuridico competente di FFS IT di valutarne l'ammissibilità dal punto di vista legale.

**2.7 Principi relativi all'utilizzo delle password (punto 4.1, K 400.9)**

Tramite la password, il sistema IT può verificare l'identità degli utenti e conferire loro l'accesso alle informazioni (dati) o ai componenti IT previsti per l'utilizzo.

L'abbinamento tra User-ID e password segreta impedisce ad altre persone, che hanno un'identificazione diversa, di acquisire i diritti d'accesso dell'utente e di eseguire un accesso non autorizzato ai componenti IT.

Non è consentito violare password di terzi o anche solo tentarne la decodificazione.

Le password devono essere mantenute segrete e possono essere note soltanto all'utente autorizzato. Devono essere altresì immediatamente modificate, non appena ne vengano a conoscenza persone non autorizzate.

Le password devono essere digitate senza essere osservati. A tale scopo, il sistema o l'applicazione deve garantire che l'inserimento possa avvenire in forma criptata.

La password deve essere composta da min. 8 caratteri, di cui almeno tre appartenenti ciascuno a una delle seguenti categorie:

- lettere maiuscole
- lettere minuscole
- cifre
- caratteri speciali

Le password non devono essere facilmente decifrabili né riferirsi a dati dell'azienda, di un'applicazione IT o dell'utente come p.es. cognome, nome, targa dell'auto, numero di telefono privato. Ci si deve astenere dall'utilizzare password banali (p.es. AAAAAAAA, 12345678, ripetizione dello User-ID). Le deroghe dovute a motivi tecnici devono essere autorizzate da IT-SR.

Le password preimpostate devono essere immediatamente modificate e le password iniziali, utilizzate per il primo login a un sistema, devono essere sostituite da formulazioni personalizzate per le sessioni successive.

Le password personalizzate devono essere sostituite da nuove formulazioni a intervalli regolari (di solito ogni mese).

Se due sistemi esistenti nella rete FFS comunicano tramite utenti di sistema, il Service Coordination può assegnare alla password le proprietà «never expires» («sempre valida») e «user cannot change password» («l'utente non può modificare la password»).

Le password non devono essere salvate su tasti di funzione programmabili.

Le password di utenti privilegiati devono essere conservate sigillate in luoghi sicuri, per garantire l'accesso ai sistemi e alle applicazioni in casi di emergenza o assenza di questi utenti. Le password archiviate devono essere sempre aggiornate dal rispettivo utente. L'utilizzo con accesso di emergenza ai diritti dell'amministratore è regolato al punto A.1.8.

## **2.8 Principi relativi all'utilizzo degli account di amministratore**

Sia gli amministratori che gli utenti non possono lavorare con questo tipo di account. Gli amministratori devono operare con User-ID personali, dotati dei rispettivi diritti di amministrazione, allo scopo di garantire la trasparenza della loro attività.

Si può fare ricorso agli account di amministratore soltanto in casi di emergenza, quando nessuno degli amministratori può intervenire.

Ulteriori norme sulla gestione di account privilegiati sono disponibili nell'istruzione K 400.11 «Account privilegiati».

# **3 Disposizioni relative all'hardware**

## **3.1 Campo di regolamentazione**

Se la singola norma non si riferisce esplicitamente a un tipo specifico di apparecchio, le seguenti disposizioni riguardano i computer delle postazioni di lavoro (PC) e i terminali mobili come laptop, smartphone e simili.

## **3.2 Collocazione (punto 3 K 400.9)**

La collocazione del PC della postazione di lavoro può essere cambiata radicalmente solo previo consenso del servizio di assistenza informatica.

I terminali mobili non possono essere lasciati incustoditi durante il normale stato d'esercizio.

## **3.3 Collegamenti in rete (punto 3 K 400.9)**

Le modifiche alla configurazione di rete possono essere eseguite soltanto dal servizio di assistenza informatica.

### **3.4 Modem (punto 3 K 400.9)**

Gli utenti non possono installare modem. Restano riservati i casi in cui l'installazione di un modem sia stata richiesta dal diretto superiore al CISO e autorizzata da quest'ultimo e dal DIO competente. In presenza di un'autorizzazione, il modem deve essere installato da I-TC.

### **3.5 Accesso remoto via IPsec VPN da PC/laptop privati (punto 4.4 K 400.9)**

L'IPsec VPN si utilizza per lavori di manutenzione e configurazioni a livello di sistema, per sviluppatori (source code repository, ambienti di prova e integrazione) nonché analisi nell'ambito di eventi e incidenti. In materia vale la regolamentazione qui di seguito riportata.

Non è consentito collegare PC o laptop privati (ossia non messi a disposizione dalle FFS) a IPSEC VPN mediante il servizio di accesso remoto (RAS). Dalla presente disposizione sono esclusi gli apparecchi autorizzati dall'NSM e dal CISO delle FFS, che montano software speciali e sono necessari per la manutenzione (p.es. di componenti di rete o sistemi di server IT).

È consentito l'accesso di terzi con PC o laptop privati, non messi a disposizione dalle FFS, tramite IT WORKPLACE RAS/IT WORKPLACE RAS.

### **3.6 Salvataggio e archiviazione dei dati (punto 3.4 e 4.1 K 400.9)**

I dati immessi dal PC devono essere salvati nell'area del server assegnata a tale scopo. I dati immessi dal laptop possono essere salvati anche sui suoi dischi fissi.

Se l'utente acquisisce dati necessari anche ad altri utenti, è tenuto a riversarli - se possibile - sul server (la duplicazione consentirà di salvare automaticamente questi dati nell'ambito del backup del server).

Se l'utente non riversa quotidianamente i dati del proprio apparecchio IT sul server, dovrà provvedere di persona a un backup periodico dei record su supporti di memorizzazione mobili che, in seguito, dovranno essere etichettati e conservati in modo sicuro. L'utente viene informato sulla procedura dal servizio di assistenza informatica.

Se possibile, i dati da supporti esterni (p.es. stick USB, dischi fissi esterni) devono essere controllati per accertare che non contengano virus. L'Help Desk (tel. n. 166) nonché il servizio di assistenza informatica forniscono agli utenti supporto e consulenza su questo aspetto.

L'utente deve informarsi preventivamente sul livello di classificazione dei dati e adattare l'utilizzo dell'apparecchio.

I dati classificati come «riservati» devono essere salvati in forma codificata, non appena sia disponibile l'infrastruttura corrispondente. Fino a tale momento, i dati di questo tipo non devono essere salvati sugli apparecchi mobili.

In mancanza di autorizzazione, non si può concedere la consultazione di dati personali o classificati come «riservati».

L'archiviazione di dati presso altre ditte è consentita solo a condizione che si rispetti la procedura RfA (Request for Architecture) e che si riceva l'autorizzazione dell'RfA Board, poiché tale operazione potrebbe determinare conseguenze di portata sconosciuta per la sicurezza.

### **3.7 Protezione antivirus (punti 3.4 e 4.1 K 400.9)**

Nei locali delle FFS o di FFS Cargo si possono utilizzare soltanto PC e laptop che dispongano di un sistema di aggiornamento automatico della protezione antivirus. Se l'utente constata che tale sistema non è installato sul proprio PC o laptop, deve portarne a conoscenza il supporto utente competente.

L'utente deve garantire che il software del sistema operativo sia aggiornato all'ultima versione delle FFS e che sia dotato dei patch di sicurezza correnti delle FFS.

Se si constata o si sospetta un attacco di virus, si deve informare immediatamente l'Help Desk o il supporto utente. Nel contempo occorre staccare il computer dalla rete. La procedura successiva viene disposta dall'Help Desk o dal supporto utente.

L'esecuzione del programma antivirus non può essere interrotta dall'utente.

Il programma antivirus installato non può essere disattivato e l'apparecchio deve essere regolarmente collegato alla rete per garantire un aggiornamento delle tabelle dei virus.

Per migliorare la protezione di un apparecchio IT mobile, l'utente può collegarsi a una rete locale o installare sul proprio dispositivo un software antivirus aggiornato.

### **3.8 Protezione antivirus per collegamenti di accesso remoto (punti 3.4 e 4.1, K 400.9)**

Ogni persona che utilizza la rete di comunicazione dati delle FFS tramite un collegamento di accesso remoto (non IT WORKPLACE–RAS), deve impiegare un programma antivirus aggiornato all'ultima versione per garantire che il PC/laptop utilizzato sia sicuramente privo di virus, worm e simili prima di ogni collegamento alla suddetta rete.

Se l'utente sospetta che la rete di comunicazione dati delle FFS possa avere ricevuto un virus/worm o simili dal proprio PC/laptop, deve informarne immediatamente l'unità organizzativa IT-SR delle FFS.



IT-SR fornisce consulenza agli utenti presenti e futuri della rete di comunicazione dati delle FFS in merito all'utilizzo di un efficiente programma antivirus.

### **3.9 Comunicazione tramite reti pubbliche wireless (Public GSM, Public WLAN) (punti 3 e 4.1 K 400.9)**

Se è disponibile un meccanismo di codifica, i dati possono essere trasmessi soltanto in forma cifrata. Un meccanismo di codifica presente non deve mai essere disattivato.

### **3.10 Collegamento a reti non soggette al controllo delle FFS (p. es. Internet, WLAN private) (punti 3 e 4 K 400.9)**

Per reti non soggette al controllo delle FFS s'intendono reti di altre organizzazioni come fornitori, clienti e simili.

È vietato collegare gli apparecchi FFS a tali reti. Lo scopo di questo divieto è impedire sia l'afflusso involontario di dati dagli apparecchi FFS all'ambiente della rete esterna, sia lo scambio di eventuali programmi dannosi tra la rete esterna e gli apparecchi FFS.

È espressamente consentito collegare un apparecchio IT WORKPLACE a Internet se lo scopo previsto è l'impiego per IT WORKPLACE-RAS.

Restano riservate le concessioni eccezionali del CISO delle FFS.

### **3.11 Smarrimento e furto (punti 3 e 4.1 K 400.9)**

In caso di smarrimento/furto di terminali FFS, tale evenienza deve essere immediatamente notificata ai servizi competenti. Lo smarrimento di apparecchi di telefonia mobile deve essere comunicato al Centro di supporto telefonia mobile. Lo smarrimento di altri apparecchi deve invece essere dichiarato secondo la procedura definita dal coordinamento dell'assistenza IT.

### **3.12 Comunicazione di eventi e rischi rilevanti per la sicurezza (punti 3 e 4.1 K 400.9)**

Ogni utente dei terminali FFS è tenuto a comunicare immediatamente eventi rilevanti per la sicurezza e/o rischi individuati al responsabile dell'oggetto competente (per i progetti: capoprogetto, per gli apparecchi acquisiti tramite IT WORKPLACE: Fachbus IT WORKPLACE (IT-OM-WUS-WDM)

## **4 Utilizzo consentito di Internet**

### **4.1 Utilizzi rischiosi (punto 3.1.3 K 400.8)**

Se possibile, ci si deve astenere da ordinazioni o assegnazioni di incarichi effettuate via Internet indicando il numero di carta di credito, nonché da transazioni finanziarie (p.es. compravendita di titoli online, telebanking), poiché tali operazioni non sono raccomandate né dalle FFS, né da FFS Cargo. L'utente riconosce che tali ordinazioni/assegnazioni di incarichi e transazioni finanziarie avvengono sempre a suo rischio e pericolo e che le FFS (comprese le società affiliate nonché associazioni in qualche modo collegate, fondazioni, ecc.) e FFS Cargo (comprese le società affiliate nonché associazioni in qualche modo collegate, fondazioni, ecc.) non rispondono dei danni che ne derivano per lui.

#### **4.2 Divulgazione di dati sensibili (punto 3.1.3 K 400.8)**

Gli User-ID e le password interni dell'azienda non possono essere pubblicati su Internet, né utilizzati per effettuare il login a servizi Internet esterni (p.es. account di posta elettronica privati, login di membri).

Né le FFS, né FFS Cargo garantiscono che sia impossibile per terzi non autorizzati leggere informazioni riservate o segrete, User-ID o password non correttamente codificati secondo i sistemi più aggiornati, o in altro modo, e trasmessi via Internet.

Se possibile, l'indirizzo e l'e-mail di lavoro, nonché il nome del datore di lavoro non dovrebbero essere rivelati via Internet.

### **5 Utilizzo consentito di servizi e programmi di posta elettronica**

#### **5.1 Informazione e supporto (punto 4.4 K 400.8)**

In caso di problemi relativi all'utilizzo dei servizi di posta elettronica, gli utenti possono rivolgersi all'Help Desk competente o al servizio di assistenza informatica. Qualora dovessero insorgere dubbi sulla sicurezza delle informazioni trasmesse, l'utente può rivolgersi al servizio di assistenza informatica, alla sezione «postazione di lavoro ed e-mail» (IT-OM-WUS-WDM) delle FFS o, in caso di sospetti rilevanti in materia di sicurezza, direttamente al CISO.

#### **5.2 Utilizzo di sistemi di posta elettronica (client) (punto 4.4 K 400.8)**

Per lo scambio di e-mail di lavoro, si possono utilizzare soltanto i sistemi e i programmi di posta elettronica definiti e autorizzati a tale scopo (p.es. Exchange/Outlook). Si possono richiedere eccezioni al CISO con il consenso del superiore.

FFS SA è autorizzata a interrompere tecnicamente l'utilizzo dei sistemi di posta elettronica ad accesso generalizzato (come p.es. Hotmail, GMX, Yahoo) da PC, laptop o PDA destinati agli scopi di lavoro di FFS SA o delle sue società affiliate e a vietarne l'utilizzo parziale o totale in ambiente di lavoro.

#### **5.3 Comunicazione prudente dell'indirizzo di posta elettronica in caso di pericolo di spam (punto 4.4 K 400.8)**

È vietato indicare l'indirizzo di posta elettronica di lavoro per newsgroup, mailing list ecc. se ciò determina l'invio in massa di messaggi elettronici a scopo puramente pubblicitario.

#### **5.4 Messaggi di posta elettronica privati (punto 4.4 K 400.8)**

Se possibile, si dovrebbe riuscire a distinguere tra messaggi di posta elettronica di contenuto puramente privato o di lavoro. Per questo motivo – nel caso di messaggi di contenuto puramente privato – se possibile si dovrebbe citare espressamente o almeno fare riferimento al concetto di «privato» nell'oggetto, nel testo o come attributo. Se possibile, ogni utente deve garantire che anche la posta in arrivo di carattere puramente privato sia contrassegnata nel modo poc'anzi indicato. Ci si deve astenere dal salvataggio e dall'archiviazione locale di messaggi di posta elettronica privati.

#### **5.5 Allegati/Attachment (punto 4.4 K 400.8)**

Per motivi legati alla sicurezza e all'impegno delle risorse, i documenti/file allegati non devono superare le dimensioni di 5 MB in uscita e 10 MB in arrivo.

È vietato inviare per e-mail i cosiddetti file di scherzi, animazioni, musica, freeware e/o shareware e di giochi.

#### **5.6 Invio di messaggi di posta elettronica (punto 4.4 K 400.8)**

Non è consentito inviare programmi eseguibili per posta elettronica. Fa eccezione l'invio richiesto per motivi di lavoro, purché sia autorizzato dal CISO.

I messaggi di posta elettronica, che sono stati inviati a indirizzi e-mail interni, possono essere inoltrati a indirizzi e-mail esterni solo dopo averne prima verificato i contenuti, mentre i messaggi con contenuti riservati non possono essere generalmente inoltrati a indirizzi e-mail esterni.

Non è consentito l'inoltro automatico di messaggi di posta elettronica a indirizzi e-mail esterni.

#### **5.7 Riservatezza/ Codifica (punto 4.4 K 400.8)**

Non si possono inviare informazioni classificate (spec. come riservate) (sotto forma di messaggi di posta elettronica e/o allegati agli stessi) all'esterno (dalla rete FFS) senza un'opportuna protezione.

Per la codifica si possono impiegare soltanto le procedure autorizzate dal CISO delle FFS. In caso di domande relative alle tecniche di codifica, l'utente può rivolgersi ai servizi di assistenza informatica.

### **5.8 Firma digitale (punto 4.4 K 400.8)**

Se consentito dal punto di vista legale, le procedure di firma digitale possono essere impiegate per garantire l'autenticità delle informazioni trasmesse.

### **5.9 Ricezione di messaggi di posta elettronica (punto 4.4 K 400.8)**

La posta in arrivo (ossia la mailbox) deve essere controllata dall'utente almeno una volta al giorno per verificare se sono arrivati messaggi. Per il resto vale il regolamento per il sostituto esposto al punto B.2.16. I messaggi di posta elettronica che non sono più necessari devono essere cancellati. Gli utenti, che ricevono e-mail da datori di lavoro delle FFS o di FFS Cargo con contenuti contrari alla legge o alla decenza, comunicheranno la fattispecie al loro superiore - allegando una stampa del messaggio ricevuto.

### **5.10 Posta elettronica e stipulazione di contratti (punto 4.4 K 400.8)**

Se possibile e se consentito dal punto di vista legale, i contratti elettronici devono essere stipulati apponendo la firma digitale.

### **5.11 Allegati ai messaggi di posta elettronica (punto 4.4 Z 400.8 e punto 5.1 K 400.8)**

Gli allegati ai messaggi di posta elettronica, trasmessi da mittenti non identificabili o di origine incerta, non devono essere aperti (pericolo di virus). Si deve informare il servizio di assistenza informatica con la massima tempestività sull'allegato sospetto.

### **5.12 Programmi ricevuti mediante posta elettronica (punto 4.4 K 400.8)**

I programmi trasmessi come allegato da un mittente noto al destinatario possono essere accettati, ma non eseguiti e installati dall'utente sull'hardware messo a disposizione dalle FFS, da FFS Cargo o i loro partner di outsourcing. Restano riservate le concessioni eccezionali, che comunque necessitano del consenso del CISO o del DIO competente.

### **5.13 Hoax ricevuti tramite posta elettronica (punto 4.4 K 400.8)**

I messaggi di posta elettronica che contengono allarmi non pertinenti (quasi sempre su virus) e l'invito all'inoltro devono essere ignorati dagli utenti. Il servizio di assistenza informatica deve essere portato a conoscenza dell'arrivo di hoax.

### **5.14 Regolamento per il sostituto (punto 4.4 K 400.8)**

Nel caso di assenza prolungata dell'utente il superiore definisce chi debba leggere e in seguito cancellare i messaggi di posta elettronica che gli arrivano nel frattempo.

L'utente deve autorizzare il sostituto ad accedere ai messaggi di posta elettronica presenti nella mailbox per la durata della sua assenza.

### **5.15 Salvataggio/Archiviazione (punto 4.4 K 400.8)**

Per motivi di sicurezza, le e-mail e i loro allegati non possono essere salvati o archiviati localmente con il programma di posta elettronica (p.es. Outlook).

### **5.16 Controllo (punto 4.4 K 400.8)**

IT-SR è autorizzata a controllare il traffico di posta elettronica verificando, con controlli anonimi a campione in base a orari definiti e per una durata limitata, che sia rispettato il punto 4.1 dell'istruzione «Utilizzo di Internet».

Nell'ambito del controllo, IT-SR deve attenersi alle disposizioni attuali della «Guida relativa alla sorveglianza dell'utilizzazione di Internet e della posta elettronica sul posto di lavoro» dell'Incaricato federale della protezione dei dati (IFPDT).

Nel caso in cui si constati un abuso, è possibile eseguire un'analisi del protocollo d'utilizzazione riferito alla persona. Il risultato di tale analisi deve essere comunicato da IT-SR al superiore della persona colpevole. Il superiore prende le necessarie misure di condotta. I responsabili del personale assegnati sono a disposizione del superiore per assistenza e consulenza.

Non possono essere applicati sistemi di controllo e supervisione volti a controllare il comportamento dei lavoratori sul posto di lavoro. In caso di necessità di sistemi di controllo e supervisione per altri motivi, essi devono essere disposti e configurati in modo da non compromettere lo stato di salute e la libertà di movimento dei lavoratori (art. 26 OLL 3).

In caso di dubbio sull'ammissibilità di un controllo, IT-Security chiederà preventivamente una consulenza legale interna delle FFS.

## 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
2-0	1.1.2013	Tutti	Istruzione acquisita nel modello attuale del regolamento; adeguamenti formali. Passaggio da K-IT a IT.