CENTRO AGROALIMENTARE ROMA SCPA

REGOLAMENTO GENERALE PER L'UTILIZZO DELLA RETE TELEMATICA E DEGLI APPARATI

03/03/2026 - ver. 7.0

Premessa

Il Centro Agroalimentare Roma C.A.R. S.c.p.A. riconosce il ruolo centrale e strategico delle reti informatiche e tecnologiche come strumenti essenziali per il funzionamento, il miglioramento dei servizi offerti e per il perseguimento dei propri obiettivi amministrativi e gestionali.

C.A.R. S.c.p.A., nel favorire l'uso delle reti da parte di tutte le sue componenti istituzionali, emana il presente Regolamento che definisce le regole per la gestione e l'utilizzo dei servizi delle reti del CAR (Centro Agroalimentare Roma).

Indice

Articolo I. Definizioni e premesse

1. La rete di trasmissione dati del CAR rappresenta lo strumento di collegamento delle risorse informatiche distribuite nel campus, aderenti agli standard[1], connesse ai sistemi informativi, ai sistemi fonia ed alla rete internazionale Internet;
2. Attraverso la rete sono collegate tutte le infrastrutture di erogazione dei servizi primari e strategici di C.A.R. S.c.p.A. e del Campus CAR. Le infrastrutture dei servizi primari, in elenco indicativo sono la rete dati ICT, la rete elettrica, la rete idrica, rete videosorveglianza e tutte le infrastrutture ad esse connesse;
3. C.A.R. S.c.p.A. sviluppa e gestisce le reti per le strutture amministrative e gestionali. Per "strutture" si intendono tutti gli stabili e le aree interne al campus del CAR;
4. Sulla rete trasmissione dati del CAR vengono erogati i servizi ai dipendenti di C.A.R. S.c.p.A. ed a tutte le aziende interne al campus (fonia e dati); inoltre, viene utilizzata per tutti i servizi interni (sicurezza, manutenzione, videosorveglianza, rete elettrica, ecc.); l'utilizzo della rete è regolato dagli articoli seguenti e dalle decisioni degli Organi di Gestione, adottate in conformità al presente regolamento e nel rispetto delle norme di legge vigenti.

Articolo II. Strutture collegate alla rete di trasmissione del CAR

Sono collegate alle reti del CAR:

1. Strutture interne, amministrative e gestionali di C.A.R. S.c.p.A., nel rispetto del presente regolamento;
2. Soggetti partecipati da C.A.R. S.c.p.A. richiedenti il collegamento, nel rispetto del presente regolamento;
3. Enti esterni a C.A.R. S.c.p.A.. Le modalità di connessione saranno disciplinate da una convenzione, sottoscritta tra le parti ed approvata dalla Direzione di C.A.R. S.c.p.A., comprovante la collaborazione e l'utilità del collegamento. Gli enti esterni non potranno accedere alla rete del CAR se non preventivamente autorizzati e collegati dal settore preposto;
4. Clienti e fornitori secondo i contratti definiti e sottoscritti di volta in volta.

Articolo III. Utenti della rete di trasmissione di C.A.R. S.c.p.A.

Possono avere accesso alla rete di trasmissione del CAR per scopi amministrativo-gestionali, compatibilmente con le risorse disponibili:

1. Il personale C.A.R. S.c.p.A. e le aziende esterne;
2. I consulenti a contratto, i consulenti visitatori, i collaboratori esterni impegnati nelle attività istituzionali svolte da C.A.R. S.c.p.A., per il periodo di tempo necessario all'espletamento dei loro compiti all'interno del CAR, previa autorizzazione del settore preposto;
3. Le Organizzazioni Sindacali Locali riconosciute che ne facciano domanda tramite il rappresentante dell'Organizzazione Sindacale Locale che si renda responsabile dell'utilizzo della connessione e/o della casella di posta elettronica;
4. Ogni altra categoria di persone autorizzata dalla Direzione di C.A.R. S.c.p.A., che determinerà tramite l'Ufficio ICT (Digital Innovation) le regole per l'autorizzazione.

Articolo IV. Utilizzo della rete e regole di accesso

1. Qualsiasi accesso alla rete deve essere associato ad una persona fisica, la cui identità dovrà essere documentata. Alla predetta persona fisica devono essere riconducibili le attività svolte utilizzando il codice utente (username di accesso), il sistema personale, il sistema server, l'accesso remoto, l'indirizzo TCP/IP, il MAC Address;
2. La richiesta di accesso comporta l'esplicita accettazione delle norme, del presente regolamento, nonché la totale assunzione di responsabilità delle attività svolte tramite la rete. L'uso della rete è in ogni caso soggetto alle norme di legge vigenti;
3. La rete trasmissione di C.A.R. S.c.p.A. può essere utilizzata esclusivamente per l'attività strumentale e di gestione del campus CAR;
4. Ogni utente della rete sarà identificato e sarà tenuto ad adottare le necessarie misure per non interferire con il corretto funzionamento delle comunicazioni, per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti ed evitare che le attività svolte producano disturbo o danni agli altri utenti. Ogni illecito o abuso riscontrato sarà oggetto di successivi provvedimenti sanzionatori;
5. In casi di interventi tecnici urgenti ed improcrastinabili, le connessioni alla rete potranno essere distaccate senza preavviso.

Articolo V. Abusi nell'utilizzo della rete

Costituisce abuso nell'utilizzo della rete trasmissione del CAR:

1. Qualsiasi atto che possa compromettere la sicurezza delle risorse informatiche e la riservatezza delle informazioni di C.A.R. S.c.p.A. o di altri Enti, fruibili attraverso la rete telematica;
2. L'accesso, l'utilizzazione, la distruzione, l'alterazione o la disabilitazione non autorizzata di risorse informatiche, anche per mezzo di chiavi di accesso (password, badge, ecc.) rese disponibili ad altri soggetti, nonché l'abbandono senza custodia di stazioni di lavoro già connesse a risorse informatiche riservate;
3. La duplicazione, l'archiviazione e l'uso di software su qualsiasi risorsa informatica di C.A.R. S.c.p.A. in violazione a disposizioni contrattuali;
4. L'utilizzazione per scopi d'interesse esclusivamente privato di qualsiasi risorsa informatica di C.A.R. S.c.p.A.;
5. Qualsiasi atto che, tramite la rete telematica del CAR, possa recare disturbo o danni a terzi;
6. L'uso di dati o di altre risorse informatiche per scopi non consentiti dalle norme di legge vigenti o in contrasto con quanto disciplinato nel presente regolamento.

L'uso personale della rete è tollerato purché:

1. non sia a detrimento dei compiti istituzionali;
2. non costituisca un carico avvertibile per la rete;
3. non costituisca un'attività commerciale o comunque con profitto;
4. non sia offensiva;
5. non violi le norme e le leggi in vigore.

In caso di abuso, secondo la gravità del medesimo e fatte salve le ulteriori conseguenze di natura penale, civile ed amministrativa, gli organi responsabili delle risorse informatiche potranno adottare provvedimenti che ne limiteranno l'uso.

L'inosservanza del presente regolamento o, in ogni caso, l'adozione di comportamenti che possano compromettere il funzionamento della rete, saranno segnalati all'utente che sarà richiamato al rispetto delle condizioni d'uso. Nel caso di abusi che rientrino nei punti del presente articolo saranno adottati i necessari provvedimenti urgenti, incluso il temporaneo distacco o la revoca dell'accesso alla rete dell'utente. Qualora il comportamento dell'utente violi le norme di legge e/o causi danni di qualunque natura (economici, d'immagine, violazione della privacy, ecc.) potranno essere adottati provvedimenti disciplinari, amministrativi o legali.

È assolutamente vietata la divulgazione di qualsiasi documento tecnico relativo alle reti di distribuzione dei servizi primari. Per reti di servizi primari si intendono le reti di trasmissione dati ICT, reti elettriche (MT e BT), reti idriche, rete di videosorveglianza, reti di allarme, reti di qualsiasi altra natura. Tali documenti,

contenendo informazioni sensibili, quali in elenco indicativo e non esaustivo planimetrie, schemi, unifilari, posizionamento apparati, passaggi cavi, tipologia di apparati, modalità di connessioni, informazioni tecnico/normative, ecc., sono classificati come riservati e strategicamente sensibili. L'accesso a tali documenti è altresì riservato, ed autorizzato dall' Ufficio ICT (Digital Innovation) in accordo con l'Ufficio titolare del documento (Area Tecnica).

All'Ufficio ICT (Digital Innovation) sono demandate l'applicazione delle regole tecniche di gestione della rete e la verifica dell'osservanza del presente regolamento. L'Ufficio ICT (Digital Innovation) ha il compito di pianificare, sviluppare, monitorare le infrastrutture di rete che collegano le strutture del campus CAR. L'Ufficio ICT (Digital Innovation) ha il compito di curare il mantenimento e lo sviluppo delle reti informatiche, nonché di monitorare il funzionamento delle infrastrutture delle reti principali. In caso di comprovati e gravi abusi, ed ha il compito di sottoporre l'evento al Responsabile dell'Ufficio ed al Responsabile della Privacy, di cui al successivo articolo, per l'individuazione di eventuali provvedimenti sanzionatori.

Articolo VI. Privacy, Accesso ai Dati e Riservatezza

La Sicurezza e la Privacy sono gestite tramite suddivisione degli account autorizzati ad operare come amministratori sulla rete, nel rispetto della normativa vigente.[2]

Il trattamento di eventuali dati personali effettuato mediante le infrastrutture e i servizi informatici aziendali avviene nel rispetto del Regolamento (UE) 2016/679 (GDPR) e della normativa nazionale applicabile, secondo i principi di liceità, correttezza e trasparenza, minimizzazione dei dati e limitazione della conservazione. C.A.R. S.c.p.A. adotta misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio e assicura che l'accesso ai dati e ai sistemi sia consentito solo a soggetti autorizzati, secondo ruoli e profili abilitativi. Restano ferme le informative e le policy aziendali applicabili in materia di protezione dei dati e sicurezza delle informazioni.

E' presente un account 'administrator', autorizzato ad operare sulle macchine come utente amministratore, normalmente non utilizzato per motivi di sicurezza. L'utente operativo utilizzato ed autorizzato ad operare come amministratore è l'utente 'ced'. Tali account sono autorizzati e creati per operare esclusivamente sulla rete e sugli apparati di C.A.R. S.c.p.A..

L'accesso e la gestione sugli apparati della rete del Campus è effettuata tramite gli account 'cisco' e nativi del vendor Cisco, assegnati al presidio esterno della rete.

L'utente di controllo e supervisione è nominativo e corrisponde al Responsabile ICT, il quale è autorizzato all'accesso ai log del Controller di Dominio e di Rete.

I log di sistema e di rete (es. autenticazioni, accessi, eventi di sicurezza e diagnostica) sono raccolti e trattati esclusivamente per finalità di sicurezza informatica, tutela e integrità delle infrastrutture, continuità operativa e gestione di incidenti/abusi. L'accesso ai log è consentito solo a personale espressamente autorizzato, per il tempo strettamente necessario e secondo criteri di necessità e proporzionalità, nel rispetto della riservatezza. I tempi di conservazione dei log e le modalità di consultazione sono definiti da apposite policy tecniche interne e sono limitati a quanto necessario alle finalità sopra indicate. Eventuali verifiche ulteriori sull'utilizzo delle risorse (controlli) sono effettuate solo in caso di esigenza concreta e documentata (es. anomalie, incidenti, violazioni del presente regolamento), nel rispetto della normativa vigente in materia di protezione dei dati personali e di rapporto di lavoro, nonché delle informative applicabili.

L'accesso ai Dati delle cartelle personali dei Dipendenti è subordinato alle policy di sicurezza di accesso delle cartelle e file, gestite dal File Server (Controller di Dominio). Ogni cartella è pertanto accessibile solo dal relativo account assegnato all'utente. La proprietà della cartella rimane degli utenti 'administrator', i quali sono autorizzati per gli ovvi motivi tecnici, alla gestione della stessa.

È obbligatorio e tassativo il rispetto delle prescrizioni di cui all'Art. V del presente Regolamento.

Articolo VII. Utilizzo di strumenti di Intelligenza Artificiale

È vietato l'utilizzo di strumenti di intelligenza artificiale all'interno dell'azienda. Tale divieto si fonda sulla necessità di tutelare la riservatezza e l'integrità delle informazioni aziendali, prevenendo qualsiasi rischio di fuoriuscita o divulgazione non autorizzata di dati sensibili. La protezione delle informazioni rappresenta una priorità assoluta e ogni tecnologia che potrebbe comprometterla viene esclusa per garantire la sicurezza dei processi e dei dati aziendali.

In ogni caso, è vietato inserire, caricare o condividere con strumenti di intelligenza artificiale non espressamente autorizzati dati personali, dati relativi a terzi, informazioni riservate o documenti interni (inclusi, a titolo esemplificativo, contenuti tecnici, amministrativi e contrattuali). L'eventuale utilizzo di strumenti di IA autorizzati deve avvenire esclusivamente per le finalità consentite e secondo le istruzioni dell'Ufficio ICT (Digital Innovation) e le policy aziendali applicabili; l'utente è tenuto a verificare l'accuratezza degli

output prima di utilizzarli in ambito lavorativo. Resta fermo il rispetto del Regolamento (UE) 2016/679 (GDPR) e della normativa applicabile in materia di protezione dei dati personali.

In deroga al divieto generale, su specifica autorizzazione della Direzione, possono essere individuate postazioni e funzioni dedicate alla sperimentazione controllata degli strumenti di intelligenza artificiale. Tali attività devono svolgersi nel rispetto delle policy interne di sicurezza, prevedendo rigorose misure di controllo per garantire la protezione dei dati. L'autorizzazione è concessa esclusivamente per finalità di ricerca, sviluppo o innovazione, e rimane soggetta a revoca in caso di non conformità.

Articolo VIII. Organismo per il coordinamento delle attività tecniche

Il Responsabile dell'Ufficio ICT (Digital Innovation), quale supervisore con funzioni di indirizzo, controllo e coordinamento su tutte le attività connesse alle infrastrutture ed ai servizi informatici relativi della rete CAR, si occuperà di:

- coordinare l'Ufficio ICT (Digital Innovation) per quanto attiene le attività inerenti alla gestione e allo sviluppo della rete trasmissione di C.A.R. S.c.p.A. e di intraprendere eventuali piani di sviluppo;
- individuare i provvedimenti sanzionatori da proporre agli Organi di Gestione, definendo le azioni tecniche da intraprendere nei casi di gravi abusi.

Articolo IX. Struttura della Rete

La struttura della rete del CAR è definibile come una doppia stella ridondata. Agli apparati di rete di Core e di Distribuzione sono collegati tutti gli strumenti aziendali e postazioni di lavoro. Sono inclusi negli apparati anche gli Access Point Wi-Fi e qualsiasi altro apparato riconducibile e collegabile con la rete Ethernet del CAR.La rete interna di C.A.R. S.c.p.A. è strutturata tramite server dedicati ai servizi aziendali (Autenticazione, Contabilità, Accessi, Sito Web, ecc.) ai quali sono connessi, tramite gli switch di rete, le Postazioni di Lavoro (PDL).

Articolo X. Postazioni di Lavoro

L'accesso alle PDL è vincolato all'inserimento di un Account e password, gestite dal sistema centrale di Active Directory, e rilasciate su autorizzazione dei Responsabili d'Ufficio. Nello specchietto di seguito riportato si riporta l'estratto delle policy applicate agli Account di accesso:

Account Policies		
Policies		Settings
Password Policy	Enforce password history	5 passwords remembered
	Maximum password age	60 days
	Minimum password age	0 days
	Minimum password length	8 characters
	Password must meet complexity requirements	Enabled
	Store passwords using reversible encryption	Disabled
Account Lockout	Account lockout duration	720 minutes
	Account lockout threshold	4 invalid logon attempts
	Reset account lockout counter after	30 minutes

Le PDL sono sotto la responsabilità degli utenti che vi accedono. Da ogni PDL è possibile accedervi con qualsiasi Account. E', pertanto, fatto obbligo agli utilizzatori disconnettere il proprio Account alla fine di una sessione di lavoro, bloccare la postazione in caso di allontanamento temporaneo (tramite la pressione della sequenza Ctrl+Alt+Canc) e spegnimento della PDL al termine della giornata lavorativa.

Sono esclusi da tale obbligo gli apparati mobile che sono assegnati personalmente.

Articolo XI. Navigazion Internet e Sicurezza PDL e Apparati Mobile

La navigazione verso Internet delle PDL è regolata da policy di sicurezza e protezione che impediscono, tramite profilazione degli account, l'accesso ai siti rientranti nelle seguenti categorie:

Adult
Adware
Astrology
Child Abuse Content
Dating
Extreme
Filter Avoidance
Gambling
Games
Hacking
Hate Speech
Hunting
Illegal Activities
Illegal Downloads
Illegal Drugs
Lingerie and Swimsuits
Non-sexual Nudity
Peer File Transfer

Pornography	Terrorism and Violent Extremism
Regional Restricted Sites (Italy)	Tobacco
Social Networking	Weapons

Eventuali autorizzazioni diverse, dovranno essere autorizzate ufficialmente dal Direttore Generale e/o Direttore Operativo.

Gli apparati mobile non sono protetti dalla navigazione internet e l'uso corretto è rimandato alla responsabilità dei singoli utilizzatori. E' facoltà dell'Ufficio ICT (Digital Innovation) richiedere l'installazione di software di sicurezza anche su apparati privati. I software saranno forniti dal medesimo ufficio.

La sicurezza generica delle PDL e degli apparti mobile è effettuata tramite un sistema Antivirus centralizzato che mantiene aggiornato e controlla costantemente la presenza di malware sugli apparati.

Articolo XII. Backup e Recovery

I Server ed i dati conservati nello Storage di Domino, sono replicati e conservati su più sistemi di Backup, NAS ed a nastro, presso il Centro Ingress, dove è realizzata una seconda sala CED dedicata alla ridondanza dei servizi ed al Backup.

Le policy applicate e i backup effettuati sono indicati nelle tabelle di seguito riportate:

Backup

Symantec Backup Exec 2012 (Appliance)

Server	Tipo	Dati	Schedulato		Conservato
FileServer	Full	S:*.*	Sabato	14:00	8 Settimane
	Incremental	S:*.*	Lun. - Ven.	13:00	8 Settimane
	Incremental	S:*.*	Lun. - Ven.	19:00	8 Settimane
FS03	Full	D:\Ced*.*	1° Mercoledì	23:00	8 Settimane
	Incremental	D:\Ced*.*	3° Mercoledì	23:00	8 Settimane
SRV-Mdaemon	Full	C:\Mdaemon*.*	Domenica	13:00	8 Settimane
	Incremental	C:\Mdaemon*.*	Lun. - Sab.	13:00	8 Settimane
	Incremental	C:\Mdaemon*.*	Lun. - Sab.	19:00	8 Settimane
SRV-Symantec	Full	C:\Drscripts*.*	Lun. - Dom.	8:15	2 Settimane
		C:\Program Files\Symantec\Backup Exec\PrepareBEDBRecovery.bat			
		C:\Program Files\Symantec\BEAppliance\Scripts\hostmgt.pl			
		D:\BackupExec\BEDB\BEDB.bak			
SM-QlikView	Full	C:\Amministrazione*.*	Mercoledì	6:30	4 Settimane
		C:\QlikView*.*			
	Incremental	C:\Amministrazione*.*	Lun. - Mar.	5:00	2 Settimane
		C:\QlikView*.*	Gio. - Dom.		

Backup								
		Server	Tipo	Dati	Schedulato		Punti ripristino	
Rubrik Air 5.3.0-p3-18540 (Virtual Appliance)	SQL Server DBs	SRV-Sql	Incremental	master	3	ogni 8 ore	3 giornalieri 1 giornaliero	3 giorni 7 giorni
				model	3	ogni 8 ore	3 giornalieri 1 giornaliero	3 giorni 7 giorni
				msdb	3	ogni 8 ore	3 giornalieri 1 giornaliero	3 giorni 7 giorni
				HRZUCCHETTI	3	ogni 8 ore	3 giornalieri 1 giornaliero	3 giorni 7 giorni
				HRZUCCHETTI_DWH	3	ogni 8 ore	3 giornalieri 1 giornaliero	3 giorni 7 giorni
	Nutanix	DC01	Incremental		1	Martedì	3 settimanali	13 giorni
		DC02	Incremental		1	Martedì	3 settimanali	13 giorni
		SM-Produzione	Incremental		1	Mercoledì	3 settimanali	13 giorni
		SM-QlikView	Incremental		1	ogni giorno	1 giornaliero 1 ultimo giorno del mese	7 giorni 1 mese
		SM-Siglaws	Incremental		1	Venerdì	3 settimanali	13 giorni
		SM-Sviluppo	Incremental		1	Mercoledì	3 settimanali	13 giorni
		SRV-Manutenzione	Incremental		1	Venerdì	3 settimanali	13 giorni
		SRV-Sql	Incremental		1	ogni giorno	1 giornaliero	7 giorni
		Vamweb4.1	Incremental		1	Venerdì	3 settimanali	13 giorni
		Zucchetti	Incremental		1	Venerdì	3 settimanali	13 giorni
		ZucchettiFE	Incremental		1	Venerdì	3 settimanali	13 giorni
	VMWare	Libraesva ESG 5	Incremental		1	ogni giorno	1 giornaliero	7 giorni

Backup						
	Server	Tipo	Schedulato		Punti ripristino	
Veeam Backup & Replication 12	Nutanix VM	DC01	Active Full	1° Venerdì	20:00	4
			Incremental	Venerdì	20:00	
		DC02	Active Full	1° Venerdì	20:00	4
			Incremental	Venerdì	20:00	
		SM-Oracle	Active Full	Giovedì	19:15	14 giorni
			Incremental	Ven. - Mer.	19:15	
		SM-Produzione	Active Full	1° Lunedì	20:00	4
			Incremental	Lunedì	20:00	
		SM-QlikView	Active Full	Domenica	19:15	14 giorni
			Incremental	Lun. - Sab.	19:15	
		SM-Sviluppo	Active Full	1° Lunedì	20:00	4
			Incremental	Lunedì	20:00	
		SRV-Kaspersky	Active Full	1° Mercoledì	20:00	4
			Incremental	Mercoledì	20:00	
		SRV-Manutenzione	Active Full	1° Mercoledì	20:00	4
			Incremental	Mercoledì	20:00	
		SRV-Mdaemon	Active Full	Sabato	0:00	14 giorni
			Incremental	Dom. - Ven.	0:00	
			Incremental	Dom. - Sab.	12:00	
		SRV-Sigla	Active Full	1° Mercoledì	20:00	4
			Incremental	Mercoledì	20:00	
		SM-Siglaws	Active Full	Domenica	20:00	4
		SRV-Sql	Active Full	Martedì	19:15	14 giorni
			Incremental	Mer. - Lun.	19.15	
		Vamweb4.1	Active Full	Domenica	20:00	4
		Wsus	Active Full	1° Venerdì	20:00	4
			Incremental	Venerdì	20:00	
		Zucchetti	Active Full	Domenica	20:00	4
		ZucchettiFE	Active Full	Domenica	20:00	4
	File Share	Fileserver	Incremental	Giornaliero	08:00	28 giorni
		Fsnxprod02	Incremental	Giornaliero	10:00	28 giorni

Articolo XIII. Apparati Informatici e Telematici

Gli apparati informatici e telematici di C.A.R. S.c.p.A., quali, Personal Computer, Notebook, Cellulari e Smartphone, SIM, Apparati di connessione remota, ecc., saranno forniti al personale quali strumenti di lavoro in relazione a quanto disposto dalla Direzione di C.A.R. S.c.p.A.. Tali strumenti dovranno essere utilizzati e conservati prestando la massima cura e ricordando che sono di proprietà aziendale. Gli strumenti forniti saranno richiesti dai Responsabili di Area e saranno calibrati secondo modalità tecniche, stabilite dall'Ufficio ICT (Digital Innovation), in funzione della destinazione d'uso e delle attività svolte dal dipendente a cui andranno fornite ed autorizzati dal Direttore Operativo e/o Direttore Generale.

La sostituzione di tali apparati verrà effettuata per valide motivazioni esclusivamente tecniche quali, in maniera non esaustiva, guasti, variate esigenze di destinazione che necessitino di apparati totalmente diversi, obsolescenza. Nello specifico l'obsolescenza tecnica di un apparato, verificata e confermata in ogni caso dall'Ufficio ICT (Digital Innovation), è per convenzione di 3 anni per apparati quali cellulari e similari e 5 anni per Notebook o PC che non svolgano funzioni tecniche avanzate e/o di managing e monitoring della rete o di altri apparati. Questi ultimi strumenti, in cui sono inclusi anche cellulari e smartphone con funzioni avanzate (di cui sia accertato l'utilizzo) oltre a Notebook e PC, hanno tempi di obsolescenza di 1-2 anni per i primi e di 3 per i secondi. In ogni caso, per la sostituzione è necessaria la richiesta dell'Responsabile dell'Ufficio e la valutazione tecnica dell'Ufficio ICT (Digital Innovation) che comunicherà, per iscritto, tale richiesta al Direttore Operativo e/o Direttore Generale che autorizzeranno l'eventuale sostituzione. Sono esclusi da tali considerazione i server e gli apparati del CED che sono sostituiti o aggiornati in funzione delle necessità di calcolo o di storage richiesto dai servizi caricati su di essi e, comunque, su supervisione e monitoraggio del personale del CED.

Su richiesta dei Responsabili d'Ufficio sarà possibile riscattare gli apparati utilizzati al prezzo determinato dall'ammortamento contabile e/o dall'oggettivo prezzo di mercato del bene, solo quando ne sia sancita l'obsolescenza per l'utilizzo aziendale, cioè quando l'Ufficio ICT (Digital Innovation) non ritenga sia possibile o necessario il riutilizzo. Il Responsabile dell'Ufficio ICT (Digital Innovation) produrrà un documento dove indicherà il prezzo e lo stato del bene, documento che sarà comunicato al Direttore Operativo e/o Direttore Generale che autorizzeranno il riscatto.

E', infine, possibile la Portability dei numeri aziendali nel caso in cui un dipendete termini il contratto di lavoro con l'azienda e voglia mantenere il numero

assegnato. E' possibile anche la Portability contraria, cioè un nuovo dipendente a cui venga assegnata una SIM, voglia mantenere il suo numero privato.

Articolo XIV. Attuazione e variazioni

Il presente regolamento, inizialmente in vigore dalla data 01/01/2015, è valido nella sua ultima versione rilasciata, aggiornata e modificata su richiesta dell'Ufficio ICT (Digital Innovation) e/o quando necessario per motivi di adeguamento delle regole di sicurezza, previa validazione del Responsabile dell'Ufficio referente del settore e validazione del Responsabile Qualità.

---

[1] Tutti i prodotti e le reti realizzate sono conformi agli standard nazionali ed internazionali. In particolare, gli standard presi in maggiore considerazione, poiché internazionalmente riconosciuti ed attuati, sono (e successive revisioni):

- ANSI/TIA-568 (serie) – Generic Telecommunications Cabling for Customer Premises (cablaggio strutturato per edifici e ambienti affini)
- ANSI/TIA-569 (serie) – Telecommunications Pathways and Spaces (percorsi e spazi per TLC)
- ANSI/TIA-570 (serie) – Residential Telecommunications Infrastructure Standard (residenziale e small office)
- ANSI/TIA-607 (serie) – Telecommunications Bonding and Grounding (Earthing) (messa a terra e collegamenti equipotenziali)
- ANSI/TIA-606 (serie) – Administration Standard for Telecommunications Infrastructure (amministrazione/etichettatura)
- ISO/IEC 11801 (serie) – Information technology — Generic cabling for customer premises (in particolare ISO/IEC 11801-1 e parti applicabili)
- EN 50173 (serie) – Information technology — Generic cabling systems (in particolare EN 50173-1, recepita in Italia come CEI 306-6, e parti applicabili)

Inoltre, nella scelta dei materiali, sono state tenute in considerazione le seguenti raccomandazioni:

- tutti i materiali e gli apparecchi impiegati sono adatti all'ambiente in cui vengono installati e sono tali da resistere alle azioni meccaniche, corrosive, termiche o dovute all'umidità, alle quali potrebbero essere esposti durante l'esercizio;
- tutti i materiali impiegati hanno dimensioni e caratteristiche tali da rispondere alle norme CEI ed alle tabelle CEI-UNEL attualmente in vigore;
- in particolare, tutti gli apparecchi ed i materiali installati sono muniti del contrassegno IMQ (marchio italiano di qualità) che ne attesti la rispondenza alle normative vigenti oppure essere comunque muniti di Marchio di Qualità riconosciuto a livello internazionale.

Nella realizzazione delle reti sono stati tenuti in considerazione i requisiti definiti per la compatibilità elettromagnetica (EMC) di una linea di trasmissione che sono raggruppati in appositi standard facenti capo ad indicazioni FCC (Federal Communications Commission) o EN (European Norm). Sono, infatti, limitati sia l'energia radiante, che potrebbe interferire con altri dispositivi elettronici presenti nell'area, nonché gli effetti dell'energia incidente, che potrebbe generare rumore sul cavo.

Le reti sono realizzate con fibre ottiche monomodali (OS1/OS2) o multimodali (OM3/OM4), secondo necessità progettuali, e con cavi in rame di tipo UTP Cat 5e o Cat 6/Cat 6A, rispettando l'applicazione dei principali accorgimenti di installazione quali:

- i cavi sono installati in modo tale che non si creino piegature o curvature eccessive;
- i cavi sono installati senza giunti da un punto all'altro;
- i cavi sono utilizzati con il minimo di trazione;
- i cavi non sono posati direttamente all'interno di controsoffittature o pannelli senza appositi cavidotti, o legati a cavi di sospensione del sistema di illuminazione;
- i cavi sono identificati con etichette;

[2] GDPR e D.Lgs. 101/2018

Il Responsabile Digital Innovation

Ing. Massimo Caldari

(firmato in originale)

Visto Referente CSIRT

Ing. Massimo Caldari

(firmato in originale)

Visto Referente Qualità

Dott. Agr. Flavio Pezzoli

(firmato in originale)