

**PROCEDURE PER IL CORRETTO UTILIZZO DI STRUMENTAZIONE INFORMATICA ALL'INTERNO DEI SITI DEL GRUPPO FCA (REGIONE EMEA)**

In linea con le Policy del Gruppo FCA e con i principi del Codice di Condotta, vengono definiti di seguito i requisiti e le responsabilità per l'uso appropriato di software ed hardware aziendali con lo scopo di prevenire comportamenti che possano danneggiare le attività del Gruppo FCA, i beni di sua proprietà o la sua immagine o che possano compromettere la sicurezza delle informazioni aziendali o violare le normative applicabili (quali a titolo esemplificativo Copyright, Privacy, ...)

Tutte le policy di riferimento per l'utilizzo delle informazioni e degli asset informatici aziendali sono reperibili sul portale fornitori.

Il legale rappresentante interessato dovrà rendere edotti i propri collaboratori della presente procedura.

**Assets informatici di FCA**

Si definisce Asset informatici qualunque device o strumentazione informatica atta ad accedere o interagire con i servizi informatici ed informativi di FCA quali a titolo esemplificativo laptop, desktop, smartphone, tablet e wearable (inclusi IoT).

Gli Asset informatici di FCA sono forniti con sistemi di protezione e configurazioni che non devono essere compromessi o modificati in alcun modo. L'utilizzo degli asset deve essere conforme alle policy aziendali, normative applicabili.

Pertanto è severamente vietato:

- Alterare la configurazione della postazione e/o inserire supporti rimovibili (comprese chiavette USB) non autorizzati. In particolare prima di accedere alla postazione è necessario verificare la presenza di chiavette USB e/o eventuali altri supporti rimovibili e se presenti richiedere l'assistenza del supporto locale ICT.
- Installare e/o disinstallare software sugli Asset informatici senza previa autorizzazione dell'ICT locale;
- Utilizzare gli Asset informatici per finalità non conforme al business di FCA;
- Utilizzare gli Asset informatici in modo o per finalità illecite e/o non conformi alle normative e leggi locali;
- Lasciare incustoditi, anche se solo temporaneamente, gli Asset informatici mobili
- Utilizzare funzionalità degli Asset informatici per scattare fotografie e/o registrare filmati o audio all'interno degli stabilimenti e degli uffici FCA (se non espressamente autorizzati da Sicurezza Industriale);

Inoltre è necessario:

- Segnalare tempestivamente all'ICT locale la presenza di comportamenti sospetti, inclusi, ma non solo, la presenza di virus informatici o comportamenti anomali della strumentazione informatica o nel suo utilizzo;
- Selezionare e custodire accuratamente le credenziali di accesso per accedere ai sistemi di FCA cui si è autorizzati, conformemente alle policy aziendali (lunghezza e complessità della password

devono essere conformi alle regole di FCA). Nel caso in cui si abbia il sospetto che la password possa essere compromessa è necessario cambiarla tempestivamente e contattare l'ICT locale;

- Ricordarsi di attivare salvaschermo o bloccare la propria postazione quando ci si allontana anche temporaneamente;
- Utilizzare i tool per la condivisione di desktop o applicazioni prestando attenzione a non divulgare informazioni a persone non autorizzate;

### **Assets informatici personali o appartenenti ad aziende terze**

Introdurre Asset informatici personali o di aziende terze negli uffici e negli stabilimenti di FCA deve avvenire solo previa autorizzazione e secondo le modalità e le procedure del sito. L'utilizzo di tali strumentazioni deve avvenire in conformità alla normative vigenti ed essere tale da non compromettere la sicurezza delle informazioni e la strumentazione o i servizi informatici di FCA.

Pertanto è vietato:

- Connettere gli Asset personali alla rete FCA (cablata o wifi), ai servizi o a strumentazione di FCA (se non ai servizi espressamente autorizzati e secondo le procedure del sito locale);
- Copiare e/o salvare contenuti/informazioni di FCA su device personali e/o su supporti che non siano gestiti da FCA;
- Salvare e/o memorizzare informazioni riservate di FCA su supporti/aree non gestite da FCA ivi comprese eventuali credenziali di accesso a sistemi di FCA (password, PIN);
- Utilizzare le aree comuni di FCA (file server, cloud, servizi di sharing, ...) per scopi personali o per scambiare/salvare documentazione personale.
- Connettere device personali ad Asset informatici FCA (anche solo per ricaricare la batteria).
- Connettere direttamente i device a internet se connessi direttamente o indirettamente alla rete FCA
- Utilizzare funzionalità degli asset informatici per scattare fotografie e/o registrare filmati o audio all'interno degli stabilimenti e degli uffici FCA (se non espressamente autorizzati da Sicurezza Industriale);
- Connettere alla rete FCA (wifi o cablata) strumenti o software atti a compromettere o analizzare i sistemi di sicurezza o violare la privacy delle comunicazioni di FCA (quali strumenti di Vulnerability Assessment, Penetration Test, Sniffing tools, Hacking tools....);
- Introdurre in azienda device con Hotspot WIFI personali attivi (e' sempre richiesta la disattivazione all'ingresso)
- Raccogliere dati o informazioni - in forma automatizzata o manuale - su FCA, personale di FCA o attività di FCA che non sia prettamente inerente al mandato dell'attività oggetto del contratto. Al termine dell'attività i dati, relativi al mandato, dovranno essere forniti a FCA distruggendo qualsiasi altra copia. Altresì è vietato diffondere o comunicare detti dati al di fuori dei canali ed interlocutori definiti da FCA.

Inoltre è obbligatorio:

- Laddove permesso connettere un device ad un servizio (localmente o da remoto) di FCA, garantire sotto la propria responsabilità che tale device sia allineato alle regole di FCA e alle best practice in materia di sicurezza informatica quali, a titolo esemplificativo e non esaustivo, la presenza e aggiornamento del sistema antivirus, l'aggiornamento del sistema operativo e dei software installati.

- Laddove autorizzati ad accedere ai servizi FCA, garantire che ogni documento o file depositato su aree di FCA sia libero da vincoli di copyright e/o FCA abbia il pieno diritto di custodirlo/visionarlo/utilizzarlo senza violare proprietà intellettuali di soggetti terzi.

Si ricorda inoltre di evitare ogni azione che possa compromettere l'integrità, la disponibilità e la riservatezza dei sistemi informativi di FCA.

FCA si riserva di valutare eventuali mancati rispetti della presente procedura.

Per accettazione della procedura per il corretto utilizzo di strumentazione informatica all'interno dei siti del Gruppo FCA (Regione EMEA)

Data: 14 / 07 / 2020

Timbro e Firma del legale rappresentante

  
**F.E.M. S.r.l.**  
Via Ferruccio 16/A - 03010 Patrica (Fr)  
Tel-0775-830116 - Fax 0775-839345  
C.F.P. Na 0220470605 SDI MSUXCR1  
CGIAA N. 78895 del 03-05-2002