Richtlinie

Diese Richtlinie dient dazu, den verantwortungsvollen und effizienten Umgang mit Multifunktionsgeräten in unserer Organisation zu gewährleisten. Multifunktionsgeräte sind komplexe und vielseitige Arbeitsgeräte, die verschiedene Funktionen wie Drucken, Scannen und Kopieren bieten. Durch die Einhaltung dieser Richtlinie soll die ordnungsgemäße Nutzung der Geräte sichergestellt und mögliche Risiken oder Missbräuche minimiert werden.

Geltungsbereich:

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer und weitere Personen, die Zugang zu den Multifunktionsgeräten in unserer Organisation haben.

Bitte nehmen Sie an angebotenen Weiterbildungsmaßnahmen zu den Multifunktionsgeräten teil!

I. Sichere Einbindung in Netzwerke

Stellen Sie sicher, dass Multifunktionsgeräte in Netzwerke integriert werden, sodass nur autorisierte Personen darauf zugreifen können. Verwenden Sie vorhandene oder richten Sie spezielle Authentifizierungsmechanismen ein, um dies zu gewährleisten. Es ist wichtig, dass autorisierte Computer über dieses Netzwerk eine sichere und verschlüsselte Verbindung mit dem Multifunktionsgerät herstellen können.

Für die erforderlichen Einstellungen sollten Sie gegebenenfalls Rücksprache mit dem Hersteller oder dem Wartungsdienst des Geräts halten. Es ist wichtig, dass die richtigen Sicherheitsmaßnahmen getroffen werden, um den Zugriff auf das Multifunktionsgerät auf autorisierte Benutzer zu beschränken und die Verbindung zwischen den Geräten zu schützen.

II. Absicherung der E-Mail-Funktion

Wenn das Multifunktionsgerät die Funktion hat, Dokumente per E-Mail weiterzuleiten, ist es wichtig, sicherzustellen, dass nur speziell autorisierte Personen diese Funktion nutzen können. Es sollte ausgeschlossen sein, dass beliebige Personen eine beliebige E-Mail-Adresse eingeben können, um Dokumente weiterzuleiten.

Verwenden Sie den vorgegebenen Prozess in Ihrer Organisation, um solche E-Mail-Adressen freizugeben und richten Sie diese sicher ein. Es ist besonders wichtig sicherzustellen, dass Sie über Informationen zu ausscheidenden Personen informiert werden, damit Sie entsprechende Maßnahmen ergreifen können, wie beispielsweise das Sperren der entsprechenden Mailadressen.

Durch die richtige Einrichtung und Kontrolle der Weiterleitungsfunktion per E-Mail am Multifunktionsgerät können Sie sicherstellen, dass nur autorisierte Personen diese Funktion nutzen und die Weitergabe von Dokumenten kontrolliert erfolgt.

III. Absicherung von USB-Ports

Der USB-Port am Multifunktionsgerät muss so abgesichert werden, dass ausschließlich zugelassene USB-Sticks verwendet werden können, wenn dies technisch möglich ist. Falls es nicht möglich ist, einzelne USB-Sticks zu autorisieren, muss entweder die Nutzungsfunktion komplett deaktiviert werden oder es ist eine zusätzliche Autorisierung erforderlich. Diese Autorisierung ermöglicht das Übertragen von eingehenden oder vorhandenen Dokumenten zwischen dem Gerät und dem USB-Stick, beispielsweise durch Verschlüsselung der Dateien. Es ist wichtig sicherzustellen, dass der USB-Port nicht missbraucht werden kann.

Des Weiteren sollten interne Festplatten und andere Massenspeicher gemäß dem aktuellen Stand der Technik sicher verschlüsselt sein. Dadurch wird verhindert, dass unbefugte Personen auf diese Speichermedien zugreifen und Daten verarbeiten können. Es ist ratsam zu prüfen, ob vertraglich festgelegt ist, dass interne Festplatten oder andere Massenspeicher stets in der Organisation verbleiben müssen, wenn das Gerät für Wartungszwecke oder außerhalb der Organisation verwendet wird. Eine sichere Entsorgung solcher Festplatten sollte gewährleistet werden. Gegebenenfalls sollten regelmäßige Datensicherungen von den Festplatten erstellt und diese Sicherungen angemessen vor unbefugtem Zugriff geschützt aufbewahrt werden.

Durch diese Maßnahmen wird sichergestellt, dass der USB-Port des Multifunktionsgeräts keine unautorisierte Verwendung ermöglicht und dass interne Festplatten und Massenspeicher geschützt sind, um die Vertraulichkeit und Sicherheit von Daten zu gewährleisten.

IV. Absicherung der Menüeinstellungen

Sorgen Sie dafür, dass in den Menüeinträgen keine sichtbaren Informationen darüber vorhanden sind, welche Dokumente kürzlich bearbeitet wurden, sofern dies technisch möglich ist. Es ist wichtig, sicherzustellen, dass unbefugte Personen keinen Zugriff auf Metadaten haben, die mit den bearbeiteten Dokumenten in Verbindung stehen. Falls eine solche Funktion erforderlich ist, beispielsweise um befugte Dokumente später identifizieren zu können, sollte gewährleistet sein, dass die Dokumente im Menü erst angezeigt werden, nachdem die Person, die das Gerät nutzt, ihre Organisation eingegeben hat, sofern dies technisch umsetzbar ist. Es ist ebenfalls wichtig sicherzustellen, dass die Anzahl der im Menü einsehbaren Dokumente auf das absolute Minimum beschränkt ist.

Durch diese Maßnahmen wird sichergestellt, dass in den Menüeinträgen keine vertraulichen Informationen über kürzlich bearbeitete Dokumente angezeigt werden und dass die Sichtbarkeit der Dokumente im Menü auf das erforderliche Minimum reduziert wird. Dies trägt dazu bei, die Vertraulichkeit und den Schutz der Informationen zu gewährleisten und unbefugten Zugriff auf Metadaten zu verhindern.

V. Gerätewartung

Stellen Sie sicher, dass Sie entweder persönlich vor Ort sind oder über eine sichere Verbindung zugeschaltet sind, wenn Fremdwartungsarbeiten durchgeführt werden, oder treffen Sie andere Maßnahmen, um sicherzustellen, dass die Wartungstechniker keine unbefugten Handlungen vornehmen können. Es ist besonders wichtig sicherzustellen, dass

die Techniker keine unautorisierten Festplatten austauschen, auf den Speicher zugreifen oder Daten kopieren können. Nach der Wartung sollten Sie die Wartungsprotokolle überprüfen, um sicherzustellen, dass alle durchgeführten Tätigkeiten korrekt aufgeführt sind und dass die Techniker alle aufgeführten Tätigkeiten tatsächlich durchgeführt haben. Nach Abschluss der Arbeiten sollten Sie überprüfen, ob alle zuvor eingestellten Sicherheitsfunktionen weiterhin ordnungsgemäß funktionieren.

Durch diese Maßnahmen stellen Sie sicher, dass während einer Fremdwartung keine unbefugten Handlungen durchgeführt werden können. Sie verhindern unautorisierten Zugriff auf Festplatten oder Speichermedien und schützen Ihre Daten vor unerlaubtem Kopieren. Die Überprüfung der Wartungsprotokolle gewährleistet, dass alle durchgeführten Arbeiten dokumentiert sind und dass keine unbeabsichtigten Änderungen an den Sicherheitseinstellungen vorgenommen wurden.

VI. Außerbetriebnahme von Geräten

Bevor Multifunktionsgeräte außer Betrieb genommen werden, ist es von entscheidender Bedeutung, sicherzustellen und zu dokumentieren, dass sämtliche personenbezogenen und anderweitig geschützten Daten von den Geräten vollständig entfernt werden. Wenn das Gerät interne Speichermedien enthält, sollten diese ausgebaut und sicher entsorgt werden. Wenn vereinbart wurde, dass ein externer Dienstleister diese Aufgaben übernimmt, stellen Sie sicher, dass entweder eine befugte Person während des Vorgangs anwesend ist oder dass Wartungsprotokolle erstellt werden, um sicherzustellen, dass die vereinbarten Aufgaben ordnungsgemäß ausgeführt wurden.

Es ist außerdem von großer Bedeutung, dass vor der Außerbetriebnahme alle sensiblen Daten von den Multifunktionsgeräten sicher gelöscht werden. Dies schützt personenbezogene Informationen und andere vertrauliche Daten vor unbefugtem Zugriff. Sofern interne Speicher vorhanden sind, sollten diese sicher entfernt und entsorgt werden, um sicherzustellen, dass keine Daten wiederhergestellt werden können. Wenn ein externer Dienstleister mit diesen Aufgaben betraut ist, stellen Sie sicher, dass entweder eine befugte Person anwesend ist, um den Vorgang zu überwachen, oder dass detaillierte Wartungsprotokolle geführt werden, um die ordnungsgemäße Durchführung der vereinbarten Maßnahmen zu gewährleisten.