IT-Security Checkliste

Standort: Lokation:

Datum : …/…/2020 User Herr /Frau
Tel.:

Alter Client

INV . Nr: Hardware:

Hostname: Modell:
S/N:
Kommentar:

1. Telemetrie deaktivierung

□ gpedit.msc-> computerkonfiguration->Administrative Vorlagen-> Windows komponenten-> Datensammlung und Vorabversion-> Telemetrie zulassen öffnen-> Einstellung auf Aktiviert, Option auf 0 i.o. ☐ n.i.o ☐ beh. ☐

□ außerdem unter Übermittleln des Gerätenamens in Windows Diagnosedatei zulassen-> öffnen -> **deaktivieren** auswählen. i.o. ☐ n.i.o ☐ beh. ☐

□ regedit.msc ->AllowTelemetry (REG_DWORD) öffnen:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ DataCollection\ -name AllowTelemetry und auf **0** setzen i.o. ☐ n.i.o ☐ beh. ☐

□ Deaktivierung von Telemetrie-Dienst und ETW-Sessions: services.msc-> Benutzererfahrung und Telemetrie im verbundenen Modus ->Eigenschaften-> Starttyp -> **Deaktivieren** i.o. ☐ n.i.o ☐ beh. ☐

□ Registry: HKLM\System\CurrentControlSet\Services\DialogTrack\Start = **4** i.o. □ n.i.o □ beh. □

□ HKLM\System\CurrentControlSet\Control\WMI\Autologger\Autologger-DiaTrack-Listener\Start = **0** i.o. □ n.i.o □ beh. □

□ perfmon.exe->Datensammlersätze->Startereignis->Ablaufverflogungssitzungen ->Autologger-Diagtrack-Listener->Eigenschaften->Ablaufverfolgungssitzung-> **HACKEN** bei Aktiviert **entfernen** i.o. □ n.i.o □ beh. □

2. Offene Ports analysieren und schließen

☐ Verwenden folgender Netzwerkanalyse-programm wie „nmap“ oder „Wireshark“, die Ihnen sämtliche offenen TCP- und UDP-Ports anzeigen. Identifizieren offener nicht benutzte Ports können geschlossen/geblockt werden. i.o. ☐ n.i.o ☐ beh. ☐

☐ die CMD als Admin ausführen->gebe dann, netstat -na ein und drücke Eingabe alle offenen Ports Blockieren (z.B.445,139) öffnen der Client Firwall->start->Systemsteuerung->System und Sicherheit->Windows Defender Firewall->Kicke auf Erweiterte Einstellungen (als Admin ausführen)->klicke in der Linken Spalte auf ->Eingehende Regel->Neue Regel-> klicke auf Port->Weiter->TCP->Bestimmte lokale Ports und gebe 445 ein und klicke auf ->Weiter-> Wähle ->Verbindung blockieren->Weiter->Kreuze alle drei Kontrollkästchen an und klicke ->Weiter->als Name wird folgendes verwendet: Port 445 deaktiviert i.o. □ n.i.o □ beh. □

IT-Security Checkliste

3. Auto-Updatemanagement deaktivieren

☐ Services.msc-> Windows Update -> Eigenschaften-> Starttyp-> **Deaktivieret** einstellen i.o. ☐ n.i.o ☐ beh. ☐

☐ Regestry: HKLM\System\CurrentControlSet\Services\wuauserv\ Start =**4** i.o. ☐ n.i.o ☐ beh. ☐

4. Datenschutz Einstellungen:

☐ Unter Einstellung -> Datenschutz auswählen und alle aufgeführten Windows und App-Berechtigung entsprechend der regualtorischen Maßnahmen auf "**Aus**" stellen.

Windows Berechtigung

Ermögliche Apps die Verwendung der Werbe-ID….. i.o. ☐ n.i.o ☐ beh. ☐

Website den Zugriff auf die eigene Sprachliste gestatten…. i.o. ☐ n.i.o ☐ beh. ☐

Windows erlauben, das Starten von Apps nachzuverfolgen… i.o. ☐ n.i.o ☐ beh. ☐

Vorgeschlagene Inhalte in der Einstellungs-App anzeigen… i.o. ☐ n.i.o ☐ beh. ☐

Spracherkennung

Wenn Sie die Online-Spracherkennung ausschalten… i.o. ☐ n.i.o ☐ beh. ☐

Freihand- und Eingabeanpassung

Wenn dies ausgeschaltet ist, wird Ihr persönliches Eingabe-…. i.o. ☐ n.i.o ☐ beh. ☐

Diagnose und Feedback

Standard: Sendet nur Information über Ihr Gerät, die Einstellungen… i.o. ☐ n.i.o ☐ beh. ☐

Freihand- und Eingabe verbessern – Senden Sie Freihand- und… i.o. ☐ n.i.o ☐ beh. ☐

Individuelle Benutzererfahrung – Erlauben Sie Microsoft, Ihre…. i.o. ☐ n.i.o ☐ beh. ☐

Diagnosedaten anzeigen – Aktivieren Sie diese Einstellung, um… i.o. ☐ n.i.o ☐ beh. ☐

Diagnosedaten löschen – Löscht Diagnosedaten, die Microsoft (Löschen auswählen und als Administrator bestätigen) i.o. ☐ n.i.o ☐ beh. ☐

Feedbackhäufigkeit – einstellungen auf „nie“ sollte gesetzt sein i.o. ☐ n.i.o ☐ beh. ☐

Aktivitätsverlauf

Kein Hacken bei: Meine Aktivität auf diesem Gerät speichern… i.o. ☐ n.i.o ☐ beh. ☐

App-Berechtigungen

Position – Zugriff auf den Standort auf diesem Gerät zulassen i.o. ☐ n.i.o ☐ beh. ☐

Zulassen, dass Apps auf den Standort zugreifen i.o. ☐ n.i.o ☐ beh. ☐

Positionsverlauf – Löschen einmal auswählen i.o. ☐ n.i.o ☐ beh. ☐

Auswählen, welche Apps auf Ihren exakten Standort zugreifen… i.o. ☐ n.i.o ☐ beh. ☐

Kamera – Zulassen, dass Apps auf Ihre Kamera zugreifen i.o. ☐ n.i.o ☐ beh. ☐

Auswählen, welche Microsoft Store-Apps auf die Kamera zugreifen… i.o. ☐ n.i.o ☐ beh. ☐

Zulassen, dass Desktop-Apps auf Kamera zugreifen i.o. ☐ n.i.o ☐ beh. ☐

IT-Security Checkliste

Mikrofon

Zulassen, dass Apps auf Ihr Mikrofon zugreifen	i.o. ☐ n.i.o ☐ beh. ☐
Auswählen, welche Microsoft Store-Apps auf das Mikrofon zugreifen…	i.o. ☐ n.i.o ☐ beh. ☐
Desktop-Apps den Zugriff auf Ihr Mikrofon erlauben	i.o. ☐ n.i.o ☐ beh. ☐
Stimmaktivierung – Verwenden der Stimmaktivierung durch Apps…	i.o. ☐ n.i.o ☐ beh. ☐
Apps können auf Stimm… reagieren, wenn dieses Gerät gesperrt ist	i.o. ☐ n.i.o ☐ beh. ☐
Standard-App für die Headset-Taste wählen	i.o. ☐ n.i.o ☐ beh. ☐
Benachrichtigungen - Zugriff auf Benutzerbenachrichtigung..	i.o. ☐ n.i.o ☐ beh. ☐
Zugriff auf Ihre Benachrichtigungen durch Apps zulassen	i.o. ☐ n.i.o ☐ beh. ☐
Kontoinformation - Zugriff auf Kontoinformation durch Apss zulassen	i.o. ☐ n.i.o ☐ beh. ☐
Kontakte – Zulassen, dass Apps auf Ihre Kontakte zugreifen	i.o. ☐ n.i.o ☐ beh. ☐
Auswählen, welche Apps auf Ihre Kontakte zugreifen können	i.o. ☐ n.i.o ☐ beh. ☐
Kalender – Zulassen, dass Apps auf Ihren Kalender zugreifen	i.o. ☐ n.i.o ☐ beh. ☐
Telefonanrufe – Apps dürfen Telefonanrufe ausführen	i.o. ☐ n.i.o ☐ beh. ☐
Anrufliste – Zugriff auf Ihren Anrufverlauf durch Apps zulassen	i.o. ☐ n.i.o ☐ beh. ☐
E-Mail – Zulassen, dass Apps auf Ihre E-Mail zugreifen	i.o. ☐ n.i.o ☐ beh. ☐
Aufgaben – Zulassen, dass Apps auf Ihre Aufgaben zugreifen	i.o. ☐ n.i.o ☐ beh. ☐
Messaging – Zulassen, dass Apps Nachrichten lesen oder senden	i.o. ☐ n.i.o ☐ beh. ☐
Funktechnik –…, dass Apps die Funktechnik des Geräts steuern	i.o. ☐ n.i.o ☐ beh. ☐
Weitere Geräte – Mit nicht gekoppelten Geräten kommunizieren	i.o. ☐ n.i.o ☐ beh. ☐
Hintergrund-Apps – Ausführen von Apps im Hintergrund zulassen	i.o. ☐ n.i.o ☐ beh. ☐
App-Diagnose – Zugriff auf App-Diagnoseinformation auf diesem	i.o. ☐ n.i.o ☐ beh. ☐
Automatische Dateidownloads – sollte ausgegraut sein!	i.o. ☐ n.i.o ☐ beh. ☐
Dokumente – Apps den Zugriff auf Ihre Dokumentbibliothek erlauben	i.o. ☐ n.i.o ☐ beh. ☐
Bilder – Apps den Zugriff auf Ihre Bildbibliothek haben	i.o. ☐ n.i.o ☐ beh. ☐
Videos – Apps den Zugriff auf Ihre Videobibliothek erlauben	i.o. ☐ n.i.o ☐ beh. ☐
Dateisystem – Zulassen, dass Apps auf Ihre Dateisystem zugreifen	i.o. ☐ n.i.o ☐ beh. ☐

☐ In der Registry noch zusätzliche Werte auf "0" setzen:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\OneDrive "DisableFileSyncNGSC" Wert auf "0" un HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\Explorer "NoActiveDesktop ->Wert auf "0" und NoActiveDesktopChanges -> Wert auf "0" i.o. ☐ n.i.o ☐ beh. ☐

5. Cortana deaktivieren

☐ Cortana per Regestry-Eintrag abschalten.In der Registry wechseln Sie nun in der linken Leiste in den Schlüssel: HKEY_LOCAL_ MACHINE\SOFTWARE\ Policies\Microsoft\ Windows\ Windows Search und ändern dort den Wert von AllowCortana nach einem

IT-Security Checkliste

Doppelklick auf "0". Sollten der Schlüssel und/oder der Eintrag nicht existieren, dann müssen Sie diese(n) manuell anlegen. i.o. ☐ n.i.o ☐ beh. ☐

6. regelmäßige Sicherung der Datenbestände (Backups)

☐ Werden die Datenbestände regelmäßig gesichert Ja ☐ Nein ☐

☐ Werden die Sicherungsmedien gesichert aufbewahrt Ja ☐ Nein ☐

☐ Schließen Sie die Räume in Abwesenheit ab Ja ☐ Nein ☐

7. Kamera deaktivieren

☐ HEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ CapabilityAccessManager\ConsentStore\webcam] "Value"=>"**Deny**" stellen

i.o. ☐ n.i.o ☐ beh. ☐

8. Audiorecorder deaktivieren

☐ gpedit-msc-> computerkonfiguration->Administrative Vorlagen-> Windows-komponenten-> Audiorecorder-> Ausführen des Audiore-corders zulassen->öffnen-> **Deaktivieren** einstellen!

i.o. ☐ n.i.o ☐ beh. ☐

9. Microsoft Konto deaktivieren

☐ gpedit-msc-> computerkonfiguration->Administrative Vorlagen-> Windows-komponenten-> Microsoft Konten-> Benutzerauthentifizierung von MS-Konten aller Anwender blockieren->öffnen-> **Aktivieren** einstellen!

i.o. ☐ n.i.o ☐ beh. ☐

10. OneDrive deaktivieren

☐ OneDrive deaktivieren (prüfen) gpedit-msc-> computerkonfiguration->Administrative Vorlagen-> Windows-komponenten->OneDrive-> Verwendung von OD für die Datenspeicherung verhindern->öffnen-> **Aktivieren** einstellen!

i.o. ☐ n.i.o ☐ beh. ☐

11. App-Store deaktivieren

☐ Store deaktivieren (prüfen) gpedit-msc-> computerkonfiguration->Administrative Vorlagen-> Windows-komponenten->Store-> Automatisches Herunterladen und Installieren von Updates deaktivieren->öffnen-> **Aktivieren** einstellen!

i.o. ☐ n.i.o ☐ beh. ☐

12. Benutzerkontensteuerung deaktivieren

☐ UAC deaktivieren (prüfen) Geben Sie den Befehl "regedit" ein und klicken Sie auf "OK". "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, Klicken Sie doppelt auf den Eintrag "EnableLUA" und setzen Sie den Wert auf „**0**“.

i.o. ☐ n.i.o ☐ beh. ☐

TMB Health.IT

IT-Security Checkliste

13. Treibersignatur deaktivieren

☐ Fenster geben Sie den Befehl "BCDEDIT –Set LoadOptions DDISABLE_INTEGRITY_ CHECKS" **ohne** die **Anführungszeichen** ein und **bestätigen** Sie **mit** Taste „**Enter**“. Zur Deaktivierung benötigen Sie die Befehle "BCDEDIT –Set LoadOptions EENABLE_INTEGRITY_ CHECKS" und "BCDEDIT –Set TESTSIGNING OFF"

i.o. ☐ n.i.o ☐ beh. ☐

14. Treibersignatur deaktivieren

☐ UAC deaktivieren (prüfen) Geben Sie den Befehl "regedit" ein und klicken Sie auf "OK". "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, Klicken Sie doppelt auf den Eintrag "EnableLUA" und setzen Sie den Wert auf „**0**“.

i.o. ☐ n.i.o ☐ beh. ☐

16. Treibersignatur deaktivieren

☐ UAC deaktivieren (prüfen) Geben Sie den Befehl "regedit" ein und klicken Sie auf "OK". "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, Klicken Sie doppelt auf den Eintrag "EnableLUA" und setzen Sie den Wert auf „**0**“.

i.o. ☐ n.i.o ☐ beh. ☐

17. Programm-Kontrolle

☐ Geben Sie Systemsteuerung ->klicke im Fenster auf System und Sicherheit. Im Feld unter Wartungscenter klickst Du auf den Eintrag -> Einstellungen der Benutzerkontensteuerung ändern. Schiebe dort den Regler mit der Maus ganz nach oben, damit Zukunft der Anwender informiert wird, wenn Änderung Microsoft am Windows System durchführt.

i.o. ☐ n.i.o ☐ beh. ☐

18. Datenausführungsverhinderung

☐ Unter Systemsteuerung -> System-> Remoteeinstellungen ->(Admin Anmeldung gefordert) Erweitert->Leistungen-> Einstellungen-> dann auf den Reiter Datenausführungsverhinderung die Schutzfunktion von "für erforderliche Windows-Programme" auf "alle Programme und Dienste". Über den OK-Button übernehmen der Einstellung (Neustart des PC wird benörigt und wird angezeigt) fenster danach schließen und Neustart durchführen

i.o. ☐ n.i.o ☐ beh. ☐

19. Überprüfung von Sicherheitseinstellung bei Firefox

☐ Standort/Positionsdienst deaktivieren: Einstellungen -> Datenschutz & Sicherheit-> Berechtigungen ->Standort ->Einstellungen->im Kasten unterhalb des neun geöffneten Fensters in den Kasten ein Hacken setzen -> Änderung speichern

i.o. ☐ n.i.o ☐ beh. ☐

☐ Erweiters Sicherheits Plugin „Ublock Origin“ installiert?

i.o. ☐ n.i.o ☐ beh. ☐

☐ Erweiters Sicherheits Plugin „NoScript“ installiert?

i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Streng auswählen

i.o. ☐ n.i.o ☐ beh. ☐

IT-Security Checkliste

☐ Menü -> Datenschutz & Sicherheit -> Berechtigungen-> PopUp Fenster blockieren ->Hacken setzen?
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Berechtigungen-> Warnen, wenn Websites versuchen, Add-ons zu installieren ->**Hacken setzen**?
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Datenerhebung durch Firefox und deren Verwendung-> **Hacken** bitte **entfernen**?
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Websites eine "Do Not Track"-Information senden, dass die eigenen Aktivitäten nicht verfolgt werden sollen -> **immer** "auswählen"?
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Firefox wird eine Chronik "**niemals anlegen**" auswählen
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Berechtigung ->Kamera ->Einstellungen ->Neue Anfragen für den Zugriff auf Ihre Kamera blockieren Hacken setzen und **Änderung speichern**
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Berechtigung ->Mikrofon ->Einstellungen ->Neue Anfragen für den Zugriff auf Ihr Mikrofon blockieren -> Hacken setzen und **Änderung speichern**
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Berechtigung ->Benachrichtigungen ->Einstellungen -> Neue Anfragen zum Anzeigen von Benachrichtigungen blockieren -> **Hacken setzen** und Änderung **speichern**
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Berechtigung -> Automatische Wiedergabe -> Einstellungen ->Standard für alle Websites: Medien mit Audio blockieren ->auswählen -> Änderung speichern
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Berechtigung -> Virtuelle Realität ->Neue Anfragen für den Zugriff auf Ihre VR-Geräte blockieren-> Hacken setzen-> Änderung speichern
i.o. ☐ n.i.o ☐ beh. ☐

☐ Menü -> Datenschutz & Sicherheit -> Datenerhebung durch Firefox und deren Verwendung-> Hacken entfernen bei-> Firefox das Installieren und Durchführen von Studien erlauben
i.o. ☐ n.i.o ☐ beh. ☐

Hiermit bestätigen wir, dass der TMB-Eingesetzte Techniker alle Checklisten Aufgaben zur vollen Zufriedenheit geprüft hat.

Ort: Datum:

...../.....
rechtsgültige Unterschrift/Stempel /Vor-Nachname des Auftraggebers

Ort: Datum:
.....
rechtsgültige Unterschrift Techniker (MA-Nr.)