PC-Richtlinie des Landkreises Harburg und IT-kooperierender Kommunen

1. Ziel und Geltungsbereich

Nahezu alle betrieblichen Prozesse in unseren Behörden sind heute von der Nutzung der Informationstechnik abhängig.

Unsere Bürger vertrauen darauf, dass ihre Daten vertraulich behandelt und alle Maßnahmen ergriffen werden, um die Integrität und die Verfügbarkeit ihrer Daten zu gewährleisten.

Um unsere IT-Systeme sowie unsere eigenen und die Daten unserer Bürger vor versehentlichem oder vorsätzlichem Missbrauch, vor Zerstörung oder Verlust zu schützen, sind alle Benutzer verpflichtet, die Bestimmungen dieses Dokuments zu beachten.

Benutzer im Sinne dieses Dokuments ist, wer im Rahmen der Aufgabenerfüllung am Arbeitsplatz oder mobil Desktop-PC, Notebooks oder Tablets (nachfolgend zusammenfassend „PC“ genannt) einsetzt.

Die ITK Harburg (nachfolgend „IT“ genannt) betreibt alle IT-Systeme der Behörden und ist verantwortlich für die IT-Sicherheit.

2. Regelungen zur IT-Sicherheit

2.1 Der PC wird ausschließlich für dienstliche Aufgaben zur Verfügung gestellt. Private Arbeiten dürfen damit nicht erledigt werden. Gleiches gilt für das E-Mail-System und die dienstliche E-Mail-Adresse.

2.2 Die IT-Sicherheit der von der IT ausgelieferten PC wird durch ein Bündel von hard- und software-technischen sowie administrativen Instrumenten gewährleistet. Es ist generell untersagt, sicherheitsrelevante Konfigurationsmerkmale zu verändern oder zu deaktivieren.

2.3 Es darf nur unter Mitwirkung der IT beschaffte bzw. von der IT geprüfte und freigegebene Hard- und Software eingesetzt werden. Hardware darf nur an den von der IT vorgesehenen Schnittstellen betrieben werden.

2.4 Reparatur- und Diagnosearbeiten dürfen nur von Mitarbeitern der IT bzw. von durch die IT beauftragten Dritten durchgeführt werden.

2.5 Die Verwendung betriebsfremder Datenträger (USB-Stick, CD, DVD oder sonstige externe Datenträger) oder betriebsfremder PC zum Laden von Daten oder Programmen (auch Demonstrationsprogramme externer Anbieter) ist nicht gestattet.

2.6 Betriebliche externe Datenträger sind für Dritte unzugänglich aufzubewahren.

2.7 Desktop-PC dürfen nicht aus den Dienstgebäuden entfernt werden. Notebooks und Tablets sind von dieser Regelung ausgenommen. Die Benutzer sind für diesen Fall dafür verantwortlich, dass die Geräte gegen Missbrauch und Verlust geschützt werden.

2.8 Daten, die nicht zur Erfüllung dienstlicher Aufgaben erforderlich sind, dürfen nicht eingespielt werden. Ebenso dürfen Daten das Unternehmen ausschließlich zu dienstlichen Zwecken verlassen. Dies gilt für Datenträger jeglicher Art sowie für den elektronischen Datenversand.

2.9 Eigenprogrammierungen sind nur zulässig, wenn dazu die von der IT gelieferte bzw. von der IT geprüfte und freigegebene Software oder darin integrierte Module verwendet werden.

2.10 Zugangsdaten zu Systemen und Anwendungen, insbesondere Passwörter, sind für Dritte unzugänglich aufzubewahren. Die Weitergabe von Passwörtern auch zum Zweck der Vertretung ist generell untersagt.

2.11 Anmeldevorgänge am PC oder an IT-Systemen, die eine Autorisierung erfordern, sind so vorzunehmen, dass die Tastatureingaben nicht beobachtet oder aufgezeichnet werden können.

2.12 Beim Verlassen des Arbeitsplatzes ist der Bildschirm manuell zu sperren. Zusätzlich erfolgt eine automatische Sperrung des Gerätes nach einer kurzen Zeit.

2.13 System- und sicherheitsrelevante Aktivitäten der Benutzer werden protokolliert. Bei Bedarf können zum einen mögliche Fehlfunktionen analysiert, zum anderen eine missbräuchliche Nutzung nachvollzogen werden.

2.14 Alle Sicherheitsvorfälle sind unverzüglich dem Service Desk der IT (Tel.300 oder hotline@lkharburg.de) zu melden. Ein Sicherheitsvorfall ist ein unerwünschtes Ereignis, das eine Einschränkung oder den Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität von Daten und Systemen nach sich ziehen kann. Insbesondere die folgenden Merkmale deuten auf das Vorliegen eines Sicherheitsvorfalls hin:

a) Datenverlust ohne erkennbaren Grund
b) Sperrung von Zugängen ohne erkennbaren Grund
c) Meldungen des Virenscanners
d) Systemmeldungen die auf Missbrauch hinweisen
e) Funktionsverlust bei Programmen

2.15 Bei Fragen, die sich aus diesen Regelungen ergeben, steht der Service Desk der IT unterstützend zur Verfügung.

3. Gesonderte Regelungen bei Telearbeit

Die Mitarbeiter verwahren ihre Arbeitsunterlagen, Passworte, Sicherungskopien etc. so, dass unbefugte Dritte keine Einsicht nehmen können.

4. Verantwortung für den ordnungsgemäßen Einsatz

Bei groben Verstößen gegen die in diesem Dokument festgelegten Regelungen wird die IT den PC still legen und den Arbeitgeber benachrichtigen.

Für Folgen durch den Verstoß gegen diese Regelungen haften Mitarbeiter entsprechend den gesetzlichen Bestimmungen.

5. Schlussbestimmungen

Die Inhalte dieses Dokuments wirken gemeinsam mit der IT-Sicherheitsleitlinie und allen übrigen Richtlinien zur IT-Sicherheit.

Des Weiteren sind alle Benutzer verpflichtet, geltende Gesetze, Vorschriften und Regelungen, z.B. zum Datenschutz, Urheberrecht oder Lizenzregelungen zu beachten.

Sollte eine Bestimmung dieses Dokuments unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt.

erhalten: _____ _____

(Ort/Datum) (Name, Vorname)

_____

(Unterschrift des Mitarbeiters)