

# Umgang mit Passwörtern



Zentrale Projektgruppe Netze am  
Ministerium für Kultus, Jugend und Sport Baden-Württemberg

## Hinweise des Landesbeauftragten für den Datenschutz Baden-Württemberg zum Umgang mit Passwörtern - Stand: 25. Juni 2010 -

### Grundprinzip des datenschutzgerechten Passwortschutzes:

Der berechtigte Benutzer muss sich sein Passwort **leicht merken** können.

Für alle anderen muss es dagegen möglichst **schwer** sein, das Passwort **herauszufinden**.

Regel	Beschreibung	Hinweise
<b>Grundsätzlich zu beachten ist:</b>		
R1	Es sind <b>individuelle</b> Kennungen und Passwörter zu verwenden.	
R2	Ein Passwort muss <b>geheim</b> gehalten werden. Es darf nirgendwo aufgeschrieben und keiner anderen Person - auch nicht dem Systemverwalter oder dem dienstlichen Stellvertreter - mitgeteilt werden.	
<b>Wie sollte ein Passwort aussehen?</b>		
R3	<b>Triviale</b> Passwörter sind zu vermeiden.	→ wie z.B. Namen oder Vornamen, Geburtsdatum, Kfz-Kennzeichen, Telefonnummer
R4	Ein Passwort muss aus mindestens <b>zehn Zeichen</b> bestehen.	
R5	Es sollte sowohl <b>Groß-</b> als auch <b>Kleinbuchstaben</b> sowie <b>Ziffern</b> sowie mindestens ein <b>Sonderzeichen</b> (wie z.B. ?, #, !) enthalten .	→ keine Umlaute
<b>Was ist bei der Passwortverwendung zu beachten?</b>		
R6	Ein Passwort darf bei der Eingabe <b>nicht</b> am Bildschirm <b>angezeigt</b> werden.	
R7	Die Passwörter dürfen im Computer nur <b>verschlüsselt gespeichert werden</b> .	→ Windows XP, Windows 7 → Browser
R8	Die Passwortdatei ist gegen unberechtigtes Kopieren zu sichern.	→ Passworttools <a href="http://passwordsafe.sourceforge.net/">http://passwordsafe.sourceforge.net/</a> <a href="http://keepass.info/">http://keepass.info/</a>
R9	Hat ein Systemverwalter einem Benutzer ein neues Passwort eingerichtet, so muss der Benutzer dieses Start-Passwort bei seiner ersten Anmeldung ändern	paedML
<b>Was sollte bei Passwortänderung beachtet werden?</b>		
R10	Ein Passwort ist <b>regelmäßig</b> zu ändern.	päd. Netz → Admin: alle 3 Monate → Lehrer → Schüler Verwaltungsnetz → Admin: alle 3 Monate → Sekretariat / Leitung → Lehrkräfte
R11	Das neue Passwort sollte sich von den früher verwendeten unterscheiden	Empfehlung → Passwort-Historie 5
R12	Ein Passwort muss umgehend geändert werden, wenn der Verdacht besteht, dass es einer anderen Person bekannt wurde.	
R13	Passwort-Änderungen müssen von den jeweiligen Benutzern selbst durchgeführt werden können	
R14	Nach mehreren fehlerhaften Anmeldeversuchen unter derselben Benutzerkennung muss die Kennung für die weitere Benutzung gesperrt werden.	paedML
R15	Anmeldefehlversuche sind zu protokollieren	paedML



Quelle: <http://www.baden-wuerttemberg.datenschutz.de/service/dfd-merkblaetter/passwort.htm>

# Umgang mit Passwörtern

## Beispiele für Merkgeregeln:





Sichere Passwörter sollten mindestens aus 10 Zeichen bestehen!	SPsma10Zb!
Treffen der reg. Multis im Jan. 2011 an der AKA Esslingen	TdrMiJ.2adAE
Mein Geburtstag ist am 22.06.1983!	MGia2.0.1!

## Passwort – Stresstest

	Hinweis: Führen Sie den Stresstest NIE mit eigenen Passwörtern durch!	
---	---	---

## Passwort – Generatoren

<http://www.anonym-surfen.com/passwort-generator>  
<http://www.belwue.de/support/passworterzeugung0.html>

<b>Merksatz</b>	Sichere Passwörter sollten mindestens aus 10 Zeichen bestehen!	Treffen der reg. Multis im Jan. 2011 an der AKA Esslingen	Mein Geburtstag ist am 22.06.1983!	
Passwort	SPsma10Zb!	TdrMiJ.2adAE	MGia2.0.1!	
Zeichenanzahl	10	12	10	
<a href="https://passwortcheck.datenschutz.ch/check.php?lang=de">https://passwortcheck.datenschutz.ch/check.php?lang=de</a>				
 Qualität des Passworts in Punkten Schwellwert >= 80 Simulation eines Hybrid-Passwortcrackers - Anzahl benötigte Versuche	Das von Ihnen eingegebene Passwort ist <b>stark</b> .	Das von Ihnen eingegebene Passwort ist <b>stark</b> .	Das von Ihnen eingegebene Passwort ist <b>stark</b> .	
	100	100	100	
	14.620.053.469.964.636.160 14 Trillionen	25.361.108.938.443.636.548.608 25.361 Trillionen	2.664.433.640.640.960.232 2 Trillionen	
<a href="http://www.php-gfx.net/Scripte/passwortcheck.php">http://www.php-gfx.net/Scripte/passwortcheck.php</a>				
	Sicherheitsstatus: <b>Gut</b>	<b>Gut</b>	<b>Sehr Sicher</b>	
	- Die Länge Ihres Passworts (10) scheint ok zu sein!	- Die Länge Ihres Passworts (12) scheint ok zu sein!	- Die Länge Ihres Passworts (10) scheint ok zu sein!	
	- Mehr Zahlen im Passwort wären von Vorteil!		- Sie haben genügend Zahlen drin!	
	- Sie haben genügend Buchstaben drin!		- Sie haben genügend Buchstaben drin!	
	- Sie haben genügend "KLEIN" Buchstaben drin!		- Sie haben genügend "GROSS" Buchstaben drin!	
- Nutzen Sie mehr Sonderzeichen im Passwort!		- Sie haben genügend Zahlen drin!		
<a href="https://www.microsoft.com/security/pc-security/password-checker.aspx?WT.mc_id=Site_Link">https://www.microsoft.com/security/pc-security/password-checker.aspx?WT.mc_id=Site_Link</a>				
	Password: <input type="password" value="....."/> Strength: <span style="background-color: yellow;">Medium</span>	Password: <input type="password" value="....."/> Strength: <span style="background-color: green;">Strong</span>	Password: <input type="password" value="....."/> Strength: <span style="background-color: green;">Strong</span>	
<a href="http://www.cryptool-online.org/index.php?option=com_content&amp;view=article&amp;id=136&amp;Itemid=159&amp;lang=de">http://www.cryptool-online.org/index.php?option=com_content&amp;view=article&amp;id=136&amp;Itemid=159&amp;lang=de</a>				
	Auswertung: <span style="background-color: green;">83%</span> Komplexität: Sehr stark	Auswertung: <span style="background-color: green;">88%</span> Komplexität: Sehr stark	Auswertung: <span style="background-color: green;">100%</span> Komplexität: Sehr stark	
	83%	88%	100%	