

# What Your Password Policy Should Be

password:

```
<link rel="stylesheet" type="text/css" href="pn_style.css" />
<link rel="stylesheet" type="text/css" href="print.css" media="print" />
<link rel="icon" href="favicon.png" type="image/png" />
<link rel="shortcut icon" href="favicon.png" type="image/png" />
<link rel="alternate" type="application/rss+xml" href="http://f" title="Feed" />
<script language="javascript" type="text/javascript" src="json2min.js" />
<script language="javascript" type="text/javascript" src="jquery-1.4.2.js" />
<script language="javascript" type="text/javascript" src="jquery.flot.js" />
<script language="javascript" type="text/javascript" src="texcanvas.js" />
<script language="javascript" type="text/javascript" src="jquery.float.js" />
```

## Table of Contents

<b>Introduction</b>	3
<b>Recommended Password Policy Summary</b>	3
<b>But Aren't Passwords Going Away Soon?</b>	5
What About Other Types of Passwords?	5
<b>The Good and Bad of Passwords</b>	7
<b>Password Attacks</b>	8
Password Theft	11
In-Person	11
Social Engineering	13
Hackers or Malware on the Endpoint	15
Network Eavesdropping	17
Stolen Credential Databases	19
Visible in Publicly Accessible Code	20
How Many Passwords Are Stolen?	20
Password Guessing	20
User Preferences	20
Default Passwords Not Changed	21
Trying Common Passwords	22
Automated vs. Manual vs. Malware Guessing	22
Password Hash Theft and Cracking	23
Common Password Hash Algorithms	24
Password Hash Cracking Tools	25
Stealing a Password Hash Through Email	28
Unauthorized Password Reset or Bypass	29
Quantum Attacks	31
Password Attacks Conclusion	32

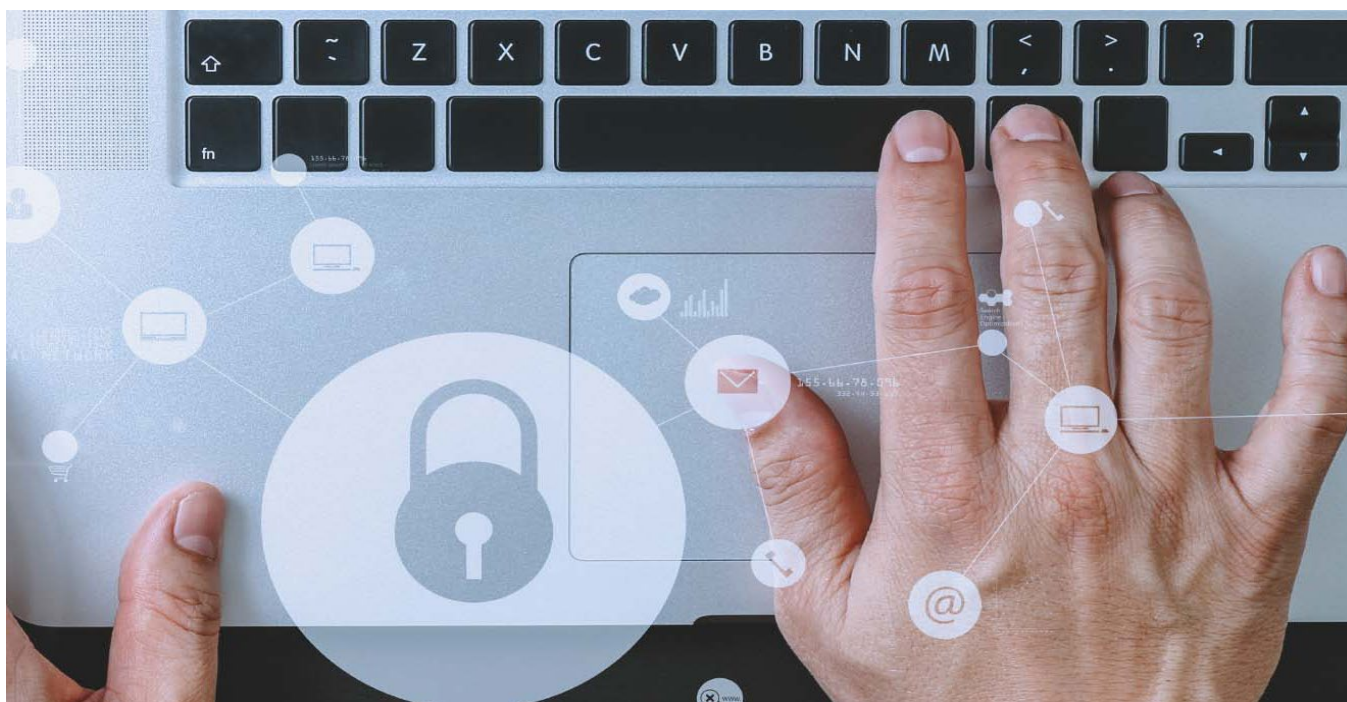
# What Your Password Policy Should Be

<b>Password Policy Attack Defenses</b>	32
What Password Attacks Care About Password Complexity	32
Minimum Password Length	34
Complexity	34
Alt-Character Passwords	34
Entropy	34
Password Testing Websites	35
Forced Password Changes	36
Not Easily Guessed	36
Use a Strong Hash	37
No Sharing	37
Emerging Technology – Keystroke Dynamics	37
Optimal Password Policy	37
<b>What Your Password Policy Should Be</b>	39
<b>Other Supporting Policies</b>	40
<b>KnowBe4 Tools</b>	41
<b>Conclusion</b>	41

# INTRODUCTION

Passwords are part of every organization's security risk profile that should be taken seriously by IT security professionals like you. Just one weak password with access to an organization's critical systems can cause a breach, take down a network or worse. Whether we like it or not, passwords are here to stay as a form of authentication for at least another decade or so. There is no time like the present to review your organization's password policy and update it for the betterment of your organization's overall security.

This whitepaper will cover the critical components of a recommended password policy for any organization around the world. It will also summarize the advantages and disadvantages of using passwords, provide a detailed breakdown of the various types of passwords attacks and defenses, as well as KnowBe4 tools that you can utilize to implement better passwords throughout your organization.



## RECOMMENDED PASSWORD POLICY SUMMARY

Your personal and enterprise passwords and policies should follow these recommendations.

The reasons your passwords and password policies should follow these recommendations are due to the methods attackers commonly use to compromise passwords and the defenses it takes to mitigate those threats.

This whitepaper will discuss the various password attacks that justify the recommended password policies. If you do not have time to read this entire whitepaper, just implement the recommended password policy to the right. But if you read this whitepaper, you will gain a good understanding of why these specific policies are recommended and why you should follow them (or not, if you decide to make a different risk decision).