מדיניות סיסמאות

במערכות ממשל זמין

גרסה 2.1

מעקב גרסאות

מס"ד	תאריך	עודכן על ידי	תיאור השינויים
1.0	11.7.2017	אופיר יהב	גרסא ראשונה
1.1	19.12.2017	אופיר יהב	עדכון לוגו
1.2	31.12.2017	אופיר יהב	עדכון סעיף 3.14 שמירת היסטוריה של 10 סמאות.
1.3	14.1.2018	אופיר יהב	עדכון סעיף 3.14 בהתאם לתו"ל רימון - שמירת היסטוריה של 20 סמאות.
1.4	10.5.2018	אופיר יהב	התאמת מדיניות הסמאות של ממשל זמין להנחיית התקשוב הממשלתי. עדכון הסעיפים הבאים: אורך הסמא של משתמש פריבילגי תהיה 14 תווים לפחות – לא 12 – היסטוריית הסמאות נשארת 20 מחזורים – על פי תו"ל רימון.
1.5	26.10.2018	אופיר יהב	תיקון שורה קטועה.
1.6	5.11.2018	אופיר יהב	חובת נעילת חשבונות במקרה של חשש לחשיפת סמאות (ר' ס' 3.32).
1.7	10.4.2020	אופיר יהב	תיקוף ועדכון המסמך – עדכון מאשרי המסמך.
1.8	22.5.2020	אופיר יהב	אין לשמור סמאות גלויות ובהזדהות מול API יש לעשות שימוש ב-TOKEN.
1.9	24.08.2020	אופיר יהב	התאמת הנוהל לדרישות פרק 15 בתקן תו"ל רימון עדכון לוגו עם המעבר למשרד הדיגיטל הלאומי.
2.0	7.11.2021	אופיר יהב	תיקוף המסמך. עדכון הלוגו עם הקמת מערך הדיגיטל הלאומי.
2.1	24.5.2022	אופיר יהב	תיקון מיספור תת-סעיפים לאורך כל המסמך.

נתוני גרסת המסמך

גורם	תפקיד	שם מלא	תאריך	חתימה
נערכה ע"י	ראש תחום מתודולוגיות הגנה בסייבר	אופיר יהב	24.5.2022	(חתימה)
נבדקה ע"י	ראש תחום אבטחת אפליקציות	אברהם ברדה	24.5.2022	(חתימה)
אושרה ע"י	מנהל מערך ההגנה בסייבר	חגי פרלמוטר	24.5.2022	(חתימה)

תוכן עניינים

1. כללי

- ממשל זמין מפתח ומספק הן מערכות פנימיות והן מערכות, מוצרים ושירותים המיועדים עבור לקוחותיו ולשימוש כלל המשתמשים אזרחי ישראל. שירותים אלו מבוססים על מערכות ומוצרים המורכבים מרכיבים חומרתיים ותוכנתיים רבים ומגוונים.
- סיסמאות הגישה אל רכיבי מערכות ומוצרים אלו – של כלל השירותים – נועדו למנוע גישה של מי שאינם מורשים לכך ובכך לשמר את מרכיבי אבטחת המידע – זמינות המידע, שלמות המידע ובראש ובראשונה חסיון המידע.
- מסמך זה נכתב בראייה כי ברוב המקרים סיסמאות הגישה אל רכיבי המערכת מנוהלות באמצעות אמצעי אוטומטי של צד שלישי.
- מסמך זה מפרט את קווי מדיניות ממשל זמין בכל הקשור לסיסמאות גישה אלו – מדיניות המהווה נגזרת של מדיניות אבטחת המידע ומדיניות פיתוח מערכות מאובטחות בממשל זמין.
- מסמך זה מהווה קובץ הנחיות כללי לניהול סיסמאות בצורה מאובטחת. המסמך נכתב בהתאם להנחיות "המכון הלאומי לתקנים וטכנולוגיה" האמריקאי (NIST).
- מסמך זה מיועד עבור מנהלי מערכות, מפתחים, מנהלי מוצר ומנהלי פרויקט המעורבים בפיתוח מערכות בממשל זמין – והם האחראים על יישום קווי המדיניות בפיתוח ותחזוקת המערכות שבאחריותם. מידת ואופן יישום ההנחיות יהיו שונים כאשר מדובר בסוגים שונים של מערכות – לדוגמא, מערכות פנימיות ומערכות לציבור הרחב – אשר להן אופי ומהות שונה והן מיועדות לקהל יעד שונה.
- הוראות מסמך זה כוללות גם את ההנחיות המפורטות בהנחיית התקשו"ב 6.2.9.2 לניהול ותפעול סיסמאות והרשאות אשר פורסמה בתאריך 1.1.2017
- מסמך זה יתוקף, יעודכן ויפורסם על ידי ראש תחום מתודולוגיות הגנה בסייבר בממשל זמין הממלא גם את תפקיד אחראי תקינה והסמכות (אחראי רגולציה) בממשל זמין.

2. קווי המדיניות בנושא הרשאות

2.1. תנאים כלליים למתן הרשאות ברשת:

2.1.1. פתיחת משתמש במערכת המידע תעשה על פי הנהלים הקיימים במשרד.

2.1.2. הבסיס למתן הרשאות גישה למשאבי מערכות מידע, הינו על בסיס תפקיד העובד(עפ"י העיקרון הצורך לדעת – Need-to-Know והמינימום הרשאות שנדרשות לצורך ביצוע עבודתו– Least Privileges).

2.1.3. לכל משתמש, יוגדר שם משתמש ייחודי.

2.1.4. לא יוגדרו "משתמשים כלליים" במערכות המידע השונות, ויבוטלו משתמשים כאלו, במידה והם קיימים.

2.1.5. עובדים זמניים – אשר קיים מועד סיום העסקה יש להגדיר את זמן תפוגת החשבון בהתאם למועד סיום העסקתו.

2.1.6. הרשאות על (משתמש פריבילגי) ליישומים מערכות יינתנו לאחר אישורו של מנהל הגנת הסייבר, שם המשתמש יהיה ייחודי ולא ניתן יהיה להשתמש בו לצורך ביצוע כניסה לרשת (ביצוע log on).

2.1.7. הרשאות על למשתמשים (משתמש פריבילגי) יינתנו לאחר אישורו של מנהל הגנת הסייבר למשתמש השייך לאגף מערכות מידע בלבד.

2.1.8. באחריות מנהל הגנת הסייבר לבקר את נושא הרשאות העל, לבדוק את הצורך של המשתמשים בהרשאות אלו ולהסיר הרשאות במידת הצורך.

2.1.9. יש לשאוף כי לכל מערכת מידע התומכת בכך – משתמש פריבילגי / מנהלן (Administrator) מערכת יזדהה עם חשבון משתמש ייעודי לניהול המערכת, השונה מזה המשמש אותו לצורך פעילות משתמש רגילה ברשת.

2.2. שינוי הרשאות – עקב שינוי תפקיד

2.2.1. משתמש שעובר תפקיד, יש לידע את אגף מערכות מידע לגבי כל עובד העובר תפקיד. בהתאם לתפקידו החדש יקבל הרשאות הנדרשות. ההרשאות הקודמות יבוטלו. היה ונידרש להשאיר את ההרשאות הקודמות לתקופה נוספת/חפיפה ההרשאות יוגבלו הזמן המערכת.

2.3. ביטול והקפאת הרשאות

2.3.1. עובד אשר צפוי להיעדר מעל שלושה חודשים יש להקפיא את הרשאותיו אלה אם אושר אחרת על פי נהלי המשרד.

2.3.2. עובד העזב את המשרד – הרשאותיו יבוטלו.

2.3.3. עובד זמני שסיים את עבודתו ,כל הרשאותיו במערכות השונות יבוטלו ,שם המשתמש יועבר למצב לא פעיל .תבוטל גישתו לרשת.

2.4. בקרת הרשאות

2.4.1. אחת לשנה מנהל הגנת הסייבר יפיק דו"ח הרשאות של כל המשתמשים במערכת על פי המחלקות ,דו"ח זה יועבר למנהלי המחלקות לבדיקה ולאישור ההרשאות הקיימות לכל עובד.

2.4.2. אחת לשנה לכל הפחות תבוצע בחינה של משתמשים פריבילגיים בהרשאות נרחבות או חריגות (בייחוד משתמשים מסוג Administrator).

2.4.3. כל כניסת משתמש למערכות המחשב במשרד תחויב בהזדהות על-ידי הקשת זיהוי משתמש וסיסמה ו\או ע"י כרטיס חכם לכל הפחות.

2.4.4. הסיסמה אישית ואיננה ניתנת להעברה.

2.4.5. נושא הגנת הסיסמאות ירוענן מעת לעת ותבוצע פעילות להגברת המודעות בתחום זה על-ידי ממונה הגנת הסייבר.

3. קווי המדיניות בנושא סיסמאות

3.1. הסיסמא לא תעבור גלויה ברשת אלא על גבי תווך מוצפן (גם hash של סיסמה לא אמור לעבור בצורה גלויה).

3.2. המערכת תספק למשתמש את היכולת להחליף את הסיסמא בעצמו, בצורה בטוחה, בכל עת.

3.3. אורכם של שמות המשתמשים של המערכת יהיה לפחות 11 תווים.

3.4. לא יוגדרו במערכת משתמשים בעלי שם משתמש טריוויאלי, כגון 'admin'.

3.5. יש למחוק משתמשים ברירת מחדל

3.6. אין לעשות שימוש בססמאות ברירת מחדל אשר הוגדרו על ידי היצרן.

3.7. המערכת תכיל בדיקה שתוודא ששם המשתמש והסיסמא יהיו שונים זה מזה ולא יכילו אחד את השני (שם המשתמש לא יהיה חלק מהסיסמא ולהיפך).

3.8. סיסמת המשתמש לא תהיה קצרה מ-10 תווים ותהייה מורכבת לפחות מ-3 קבוצות תווים, מתוך הארבע הבאות:

3.8.1. אותיות קטנות;

3.8.2. אותיות גדולות;

3.8.3. ספרות;

3.8.4. תווים מיוחדים.

3.9. סיסמתו של מנהל המערכת (אדמיניסטראטור), סיסמת משתמש על (פריבילגי) או למשתמש אפליקטיבי תהיה מורכבת מ-14 תווים לפחות.

3.10. תוקפה של סיסמת המשתמש יפוג כל 180 יום ועל המשתמש יהיה להחליף את סיסמתו בהתאם למבנה המתואר לעיל. סיסמת חשבון משתמש פריבילגי (Administrator) תוחלף מדי 90 יום.

3.11. הסיסמה לא תופיע על המסך בעת הקשתה.

3.12. אין לרשום את הסיסמה בקרבת המחשב או בכל מקום הנגיש ו/או החשוף לאחרים.

3.13. מנגנון החלפת הסיסמא ישמור היסטוריית הסיסמאות של 20 מחזורים לפחות ולא יאפשר למשתמש לחזור על אף אחת מהסיסמאות הללו בעת החלפת הסיסמא.

3.14. טרם החלפת הסיסמא על המשתמש יהיה להקיש את סיסמתו הנוכחית.

3.15. החלפת הסיסמא לא תתאפשר בטווח של 24 שעות מהחלפת הסיסמא האחרונה.

3.16. הסיסמא הראשונית של המשתמש תהייה רנדומאלית ובהתאם למבנה שהוגדר לעיל.

3.17. בעת קבלת סיסמה ראשונית, המערכת תחייב את המשתמש להחליף את סיסמתו הראשונית בעת ההתחברות הראשונה למערכת.

3.18. תוקף הסיסמא הראשונית תהיה בת יום אחד בלבד, ולאחר מכן המשתמש ינעל ולא יוכל להשתמש בה.

3.19. במקרה בו המשתמש שכח את סיסמתו, המערכת תיצור לו סיסמא חדשה. כמו הסיסמא הראשונית, סיסמא זו תהייה מוגבלת בתוקף והמשתמש יהיה מחויב להחליפה בעת השימוש הראשון בה.

3.20. יצירת סיסמא חדשה במקרה בו המשתמש שכח את הנוכחית תהייה אך ורק לאחר זיהוי המשתמש באמצעים אחרים, כגון כתובת דואר אלקטרוני, שאלות סודיות וכדומה.

3.21. מומלץ להשתמש בשילוב של השיטות כגון: שליחת מייל למשתמש עם קישור חד פעמי ומוגבל בזמן המשמש לאיפוס סיסמא, ואחרי שהמשתמש גולש הוא נשאל שאלות בטחון ואם הוא מצליח אז ניתנת לו האפשרות לשנות את סיסמתו.

3.22. אין להציג בשום שלב במחשבי המערכת, במחשבים של משתמשי המערכת, בקוד המקור של דפים וטפסים המועברים למשתמש, את מזהי האימות של המשתמשים השונים במערכת.

3.23. סיסמת המשתמש תשמר בצורת hash בבסיס המידע.

3.24. יש להשתמש באלגוריתמי Hash בטוחים כגון Sha-512 . אין השתמש באלגוריתמים לא בטוחים כגון Sha-1 ו- MD5 .

3.25. חשבונות של עובדים אשר עברו לתפקיד אחר (ואינם נדרשים עוד לעבודה עם המערכת) או עזבו את הארגון יינעלו ובהמשך יגובו ויוסרו מן המערכת.

3.26. מידי רבעון תבצע בדיקת חשבונות אשר לא נעשה בהם שימוש במשך תקופה העולה על 90 יום.

3.27. חשבון אשר לא נעשה בו שימוש במשך 90 ימים" ינעל."

3.28. חשבון ה"נעול "מעל 90 ימים(ולא הועברה דרישה לפתוח אותו מחדש) יסגר.

3.29. ברשת התקשוב המשרדית ימצא סידור להטמעת יכולות חיווי ובקרה (AUDIT) רלוונטיים.

3.30. החיווי יכלול אינדיקציה בנושא ניסיונות הזדהות כושלים ,פעילות חריגה ונתונים נוספים שיוגדרו על-ידי מנהל הגנת הסייבר.

3.31. אובדן סיסמה או חשיפתה בפני אחרים - או אף חשד לכך - יחייב את החלפתה לאלתר. כל חשבון אשר סיסמת הגישה אליו אבדה או נחשפה (או שאף קיים חשד לכך) יינעל עד להחלפת הסיסמה בחדשה.

3.32. נעילת חשבון:

3.32.1. לאחר חמישה ניסיונות הזדהות כושלים עקב הקשת סיסמה שגויה ,החשבון "ינעל "ויועבר למצב של השעיה (SUSPEND). הפעולה תירשם בקובץ חיווי (AUDIT).

3.32.2. שחרור חשבון המשתמש יתבצע רק לאחר בירור נושא החריגה ובדיקה אם מדובר בנעילה אשר התרחשה מסיבה תמימה ובלתי מכוונת או מכוונת זדון.

3.32.3. לפני פתיחת החשבון יוודאו באופן חד ערכי את זהות המשתמש .במידה וקיים ספק לגבי זהותו ,יצרו עם העובד קשר ע"י חזרה למספר הטלפון של העובד הרשום במערכת.

3.32.4. בכל מקרה של ספק או בעיה שחרורו החשבון יועבר בבדיקה ובאישור של מנהל הגנת הסייבר.

3.33. לאחר התרחשות אירוע אבטחת מידע חריג יהיה צורך בשינוי סיסמאות של חשבונות, רכיבים ושירותים - לפרטים ר' נוהל אירוע אבטחתי חריג – 1112.

3.34. טיפול בחריגות בנושא סיסמאות יועבר לטיפולם של ממונה הגנת הסייבר ו/או מנהל הגנת הסייבר בהתאם למהות החריגה .אלו יפעלו לפי נהלי המשרד בנושא זה.

4.הנחיות לשמירת סודיות הסיסמא

4.1 שמירה על סודיות הסיסמאות והגנה מפני התקפות

4.1.1. בכל מתאר סיסמאות לא יישמרו כ- HARD CODED בשום יישום, וכן לא ישמרו כ-CLEAR TEXT.

4.1.2. בהזדהות מול API המערכת תעשה שימוש ב-API Keys (Token) ולא בשם משתמש וסיסמה.

4.1.3. אין לשמור קבצים עם סיסמאות גלויות בשרת\ים.

4.1.4. יש להשתמש בהצפנה הסיסמאות ב- HASH חד כיווני.

4.1.5. יש צורך לוודא את זהות המשתמש אשר מבצע תהליך לשחזור או איפוס סיסמה, ולא לאפשר לתוקף לקבל סיסמאות של משתמשים כתוצאה מתהליך כזה או אחר.

4.1.6. יש לשמור על סודיות הסיסמאות לאורך כל הדרך (במנוחה ובתנועה).

4.1.7. במנוחה – יש לשמור על אחסון הסיסמאות בצורה מוצפנת בלבד לרבות בעת שימוש בסיסמאות בקבצי קונפיגורציה.

4.1.8. בתנועה – יש לשמור על העברת סיסמאות בצורה מאובטחת ממקום למקום בכדי למנוע התקפות MITM (Man In the Middle) ולכן יש להעביר סיסמאות באמצעות פרוטוקולים המצפינים את המידע העובר בתווך (למשל העברה באמצעות SSH ולא באמצעות FTP).

4.1.9. יש למנוע התקפות מסוג "Relay Attacks" אשר בהן התוקף הינו באמצע התעבורה ובכך ביכולתו להעביר את הסיסמה המוצפנת כמו שהיא אל מנגנון האימות ובכך אין לו צורך לבצע תהליך של "פיצוח" הסיסמה לצורך אימות למערכת. ניתן למנוע זאת על ידי שילוב מנגנון האימות עם פונקציות timestamps או עטיפת המנגנון בפרוטוקול המגן על כך כגון TLS.

4.1.10. אין לחשוף את הסיסמה אותה משתמש מזין במסך בכדי למנוע התקפות גניבת סיסמאות מסוג "shoulder surfing", ולכן יש להסתיר את הסיסמה המוזנת לדוגמה באמצעות כוכביות ולא להציגה במסך במהלך תהליך הרשמה או שחזור סיסמה.

4.1.11. ניחוש סיסמאות:

4.1.9.1 בכדי למנוע התקפות לניחוש סיסמאות יש למנוע שימוש בסיסמאות קלות לניחוש כגון שימוש בשם המשתמש כסיסמה או כל פרט

פומבי אחר הקשור לתהליך ההרשמה, שימוש בסיסמאות של חלשות בצירופי מקלדת כגון qwert, 1234!@#$

4.1.9.2 יש להגביל את מספר הניסיונות להיכנס לחשבון במרווח זמן מסוים על ידי שימוש בטכניקות כגון:

- נעילת משתמש ל-15 דק' לאחר X ניסיונות שנכשלו.
- יצירת השהיית זמן רנדומלי בין ניסיון לניסיון כך שלא יפגע בחווית המשתמש אך כן יגן על מנגנון האימות, לדוגמה יצירת השהייה של בין 10-30 שניות בין ניסיון לניסיון בצורה רנדומלית.
- מניעת חשיפת שגיאות במנגנון האימות המעידות על קיום או אי קיום משתמש.
- החזרת סטטוס קוד 200, בעת כשל בתהליך האימות כך שלא תהיה אינדיקציה על אימות תקין על סמך קוד הסטטוס החוזר מהשרת.

4.1.12. <u>"פיצוח" סיסמאות:</u>

- יש להצפין סיסמאות בהצפנה חד כיוונית בעזרת אלגוריתם חזק (לכל הפחות SHA256).
- יש להשתמש ב-salt רנדומלי לכל סיסמה הנוצרת לצורך מניעת hash זהה ליותר ממשתמש אחד (unique salt).
- אין להשתמש ב-salt זהה לכל הסיסמאות.
- אין להשתמש ב-salt המורכב מפרטי המשתמש אלא ברנדולי.
- אין להשתמש ב-salt קצר מדי היות והדבר יקל על התוקף, ההמלצה הינה שימוש ב- salt שזהה לגודל ה- hash הנוצר ביצירת הסיסמה, לדוגמה בהצפנת SHA256 הפלט הינו 32 bytes, לכן מומלץ ליצור salt רנדומלי באותו הגודל.
- הצפנה כפולה יוצרת בעיות ואינה מהווה פתרון יותר מאובטח, על כן אין להשתמש בשיטה זה.
- אין להשתמש בשיטות הצפנה שאינן מאובטחות כגון md5, base64, sha1.
- Salt צריך להיווצר בצורה רנדומלית באמצעות מנגנון המיועד לכך כגון: Cryptographically Secure Pseudo-Random Number Generator (CSPRNG), ולא בשיטות קוד פשוטות כגון rand(). דוגמה: https://msdn.microsoft.com/en-

us/library/system.security.cryptography.rngcryptoservicepro
vider(v=vs.110).aspx

- אין להשתמש בשיטות הצפנה שאינן מאובטחות כגון md5, base64, sha1.
- שמירת ה-SALT תישמר יחד עם ה- HASH בבסיס הנתונים תחת רשומת המשתמש.
- אין להשתמש בהצפנה או חשיפת ה- HASH בקוד צד לקוח.
- דוגמה נכונה ליישום ב#C:

https://crackstation.net/hashing-security.htm#aspsourcecode