# נוהל: זיהוי ואימות

**----------------------------------------------------------------------------------------**

**נספחים:** אין

 **הפניות:** חוק הגנת הפרטיות התשמ"א 1981.

 תקנות הגנת הפרטיות התשע"ז 2017.

 תקן ISO 27001:2013

**----------------------------------------------------------------------------------------**

1. **כללי**
	* 1. אוניברסיטת בן-גוריון בנגב, אשר ברשותה מערכות מידע ורשתות תקשוב, מחייבת את המשתמשים במערכות
		2. שלה להזדהות באמצעות סיסמה טרם הגישה לרשת ולמערכות המידע, וזאת לשם בקרת הגישה אל משאבים
		3. אלה.
	1.
2. **המטרה:**

מטרת נוהל זה היא לקבוע עקרונות אחידים לכלל המשתמשים בנוגע למבנה הסיסמה ועדכונה, בהלימה, בין

היתר, עם דרישות אבטחת מידע.

1. **הגדרות**

* 1. **מאגר מידע** – אוסף פרטי מידע אישי השמורים על-גבי מדיה דיגיטלית, או כל הגדרה אחרת, כפי שתהיה בחוק הגנת הפרטיות, תשמ"א-1981, מעת לעת. רשימה מעודכנת של מאגרי המידע של האוניברסיטה ניתן למצוא בנוהל ניהול מאגרי מידע.
	2. **מערכות מידע" או "מערכות-** כל מערכות המחשוב של האוניברסיטה, לרבות שרתים, תוכנות, כונני רשת, מאגרי מידע, שירותי ענן ודואר אלקטרוני.
	3. **משתמש/ים**– כל מי שמשתמש במערכות האוניברסיטה, לרבות סטודנטים, עובדים ובעלי תפקידים באוניברסיטה, עובדים זמניים, משתמש חיצוני, טכנאים ונותני שירותים.
	4. **סיסמה**- אות מוסכם המשמש אמצעי זיהוי לשם בקרת גישה למערכות המידע. הסיסמה יכולה לכלול מילה או רצף מילים, ספרות או תווים כלשהם או שילוב שלהם, הכל בהתאם למפורט בנוהל זה.
	5. **זיהוי(Identification)-** נתון המאפשר לזהות את המשתמש או הרכיב/שירות באופן חד ערכי.
	6. **אימות(Authentication)-** נתון המאפשר לאמת את זהותו של המזדהה.
1. **תוכן הנוהל**
	1. **כללי :**
		1. לכל משתמש, רכיב ושירות יוגדר זיהוי ואימות ייחודי משלו.
		2. במערכות בהם קיימים רכיבים בהם לא ניתן ליישם הזדהות כלל מסיבות טכניות או תפעוליות

 (כגון עמדון הנדרשות להיות בשימוש 24/7) נדרש ליישם בקרות מפצות שיאפשרו זיהוי בדיעבד

 של המשתמשים ברכיב(כגון צילום המתחם).

* 1. **אימות רכיבים(כגון מחשב נייח):**
		1. ככלל אימות יבוצע תוך שימוש בתעודה דיגיטלית(Certificate).
		2. במידה ושימוש בתעודה דיגיטלית אינו אפשרי, אימות יבוצע תוך שימוש בסיסמאות מורכבות

 וארוכות:

* + - 1. 14 תווים לפחות.
			2. תכיל אות קטנה
			3. תכיל אות גדולה אחת לפחות
			4. תכיל ספרה אחת לפחות
			5. תכיל תו מיוחד אחד לפחות(לדוג' %$#@!)
	1. **אימות משתמשים:**
		1. במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, כמפורט בנוהל ניהול מאגרי מידע,

 אופן הזיהוי ייעשה ככל האפשר על בסיס 2FA[[1]](#footnote-1).(סיסמה- something you know ואחד

 מהשניים: רכיב פיזי something you have או אמצעי ביומטרי- something you are).

* + 1. אורך סיסמה עבור משתמש רגיל תהיה לפחות 8 תווים
		2. אורך סיסמה עבור משתמש אדמיניסטרטיבי (Admin) תהיה לפחות 12 תווים.
		3. הסיסמה תכיל לפחות :
		4. אות קטנה אחת
		5. אות גדולה אחת
		6. ספרה אחת
		7. תכיל תו מיוחד אחד לפחות(לדוג' %$#@!)
		8. ככלל, תוקף הסיסמה יוגבל לחצי שנה, לאחר זמן זה יהיה נדרש להחליף את סיסמה, תזכורת

 תשלח חודש מראש. תזכורת נוספת תשלח שבוע מראש.

* + 1. סיסמה ללא תוקף תוקצה באופן חריג וככלל רק לצורך יצירת חשבון משתמש (user) להקמת

 מערכת בסיס נתונים, וזאת בכפוף לאישור מנהל אבטחת מידע. סיסמה זו תוחלף במידת האפשר

 אחת לשנה.

* + 1. חשבונות אדמיניסטרטיביים- תוקף הסיסמה של-חשבונות אדמיניסטרטיבים יוגבל ל- 3

 חודשים.

* + 1. תווי סיסמה יוסתרו על המסך בעת הקלדתם.
		2. לא יתאפשר למשתמש להפעיל תכונת הצג תווי סיסמה.
		3. תבוטל האופציה של "זכור סיסמה" ו-auto complete לשם המשתמש.
		4. לא ייעשה שימוש בסיסמאות קודמות בהן בוצע שימוש במערכת(לפחות 20 אחורה).
		5. החלפת סיסמה תתבצע במערכת החלפת הסיסמאות בלבד.
		6. קישור למערכת ניתן למצוא כאן: [https://tamrur.bgu.ac.il/wcp/login.php?isheb=1.](https://tamrur.bgu.ac.il/wcp/login.php?isheb=1)
		7. משתמש אשר לא יחליף סיסמה כאמור לעיל, יינעל.
	1. **הזדהות:**
		1. זיהוי משתמש לא לא יאפשר זיהוי של תפקידו באוניברסיטה כגון Admin.
		2. זיהוי למאגר מידע הנמצא באחריות ה-IT יתבסס על הזיהוי הרשתי.
		3. בהזדהות למאגר מידע במחשבים ציבוריים הפזורים באוניברסיטאות לא יוצג שם המשתמש

 הארון שביצע כניסה למערכת.

* 1. **הנחיות למשתמשי קצה:**
		1. לכל משתמש יוקצה לפחות שם משתמש אחד וסיסמה אישית אחת באמצעותם יוכל לגשת

 ולהשתמש במערכות המידע, בכפוף להרשאות שניתנו לו. הסיסמה הינה אישית וחסויה

 ולמשתמש אסור למוסרה לאחר.

* + 1. אגף טכנולוגיות חדשנות ודיגיטל רשאי לנקוט צעדים כנגד מי שפעל בניגוד לאמור לעיל, לרבות

 בדרך של חסימת הגישה והשימוש במערכות המידע.

* + 1. **למשתמשים יובהר כי לצורך שמירה על סודיות הסיסמה:**
			1. אין להשתמש בכתובת הדואר האלקטרוני של האוניברסיטה לטובת רישום באתרי אינטרנט שונים (כגון אתרי קניות, חדשות וכד') שלא לצורכי עבודה ו/או לימודים ו/או מחקר, לפי העניין.
			2. אין להשתמש בסיסמה המיועדת למתן גישה למערכות המידע בשום אתר או מערכת אחרת מחוץ לאוניברסיטה.
			3. אין למסור בטלפון פרטים מזהים וסיסמאות לאנשים לא מוכרים באופן כללי, כולל אנשים לא מוכרים שמזדהים כאנשי התמיכה של האוניברסיטה או כפועלים מטעמם.
			4. אין להשאיר פתק עם הסיסמה ליד המחשב.
			5. אין לשמור במחשב סיסמאות בקובץ טקסט/וורד/אקסל שאינו מוצפן או לשלוח אותן בדוא"ל.
	1. **בקרות וביקורת:**
		1. לאחר פרק זמן של 15 דקות ללא שימוש יינעל מסך המשתמש.
		2. לאחר 5 ניסיונות אימות כושלים יינעל חשבון המשתמש- תקפוץ התרעה במערכת ה-SIEM.
		3. בקרה על חשבונות מערכת עם סיסמאות ללא תוקף: מדי חצי שנה תבוצע בקרה על כלל

 המשתמשים עם סיסמאות ללא תוקף.

* + 1. בקרה על חשבונות אדמיניסטרטיבים: מדי שלושה חודשים תבוצע בקורת על ססמאות של

 חשבונות חזקים/ אדמיניסטרטיבים.

* + 1. הגנה מפני תקיפת כוח גס (Brute force):
			1. אימות דו שלבי
			2. הגנה באמצעות דוחות ממערכות נוספת DSP))
		2. נוהל זה ייסקר ויתוקף אחת לשנה או בכל שינוי מהותי.
1. **אחריות לביצוע:**
	1. באחריות של כל מנהל מערכת לאכוף את מדיניות הסיסמאות של מערכות המידע שבתחום אחריותו,

 בהתאם לרשום בנוהל זה.

* 1. בסמכות ואחריות מנהל אבטחת מידע לבקר ולאכוף נוהל זה.

**6. תחולה: נוהל זה תקף מיום פרסומו.**

1. 2 Factor Authentication – הזדהות באמצעות שני גורמים [↑](#footnote-ref-1)