# נוהל: הרשאות גישה למערכות מידע

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

### הפניות:

[חוק הגנת הפרטיות התשמ"א 1981](http://www.lgbtlaw.tau.ac.il/sites/default/files/field/law/file/%D7%97%D7%95%D7%A7%20%D7%94%D7%92%D7%A0%D7%AA%20%D7%94%D7%A4%D7%A8%D7%98%D7%99%D7%95%D7%AA.pdf).

[תקנות הגנת הפרטיות התשע"ז 2017.](https://bgu365.sharepoint.com/%3Ab%3A/s/GDPR-2/EZrRpDxPHrxFjs8Lq6l1xdYBzassKzPziswAjwBECzrv6g?e=bhhQPL)

[תקן ISO 27001:2013](https://bgu365.sharepoint.com/%3Ab%3A/s/GDPR-2/EY9cv0QAl0VGhM-9PnaTE2cBhuWnxVSpGtQdjkJVYsjisw?e=5k6mvs)

[GDPR](https://bgu365.sharepoint.com/%3Ab%3A/s/GDPR-2/EYKE_NFSE-tKmjpMj2QRKKgBlsdEr-bRfrrZSy6n7Iyseg?e=CdgwhL)

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

1. **כללי**

 נוהל הרשאות גישה למערכות מידע עוסק במתן גישה למערכות מידע של האוניברסיטה ובגישה למידע באופן כללי, כך שהרשאות הגישה ינוהלו בהתאם להגדרות התפקיד ובמידה הנדרשת לביצוע התפקיד.

1. **המטרה**

 מטרת נוהל זה להגדיר מדיניות בתחום ניהול הרשאות גישה למערכות המידע ולמידע באוניברסיטה.

1. **הגדרות**

* 1. **האגף- אגף טכנולוגיות חדשנות ודיגיטל .**
	2. **המחלקה- מחלקת תשתיות IT.**
	3. **מערכות מידע" או "מערכות" –** כל מערכות המחשוב של האוניברסיטה, לרבות שרתים, תוכנות, כונני רשת, מאגרי מידע, שירותי ענן ודואר אלקטרוני.
	4. **מאגר מידע** **-** אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי המיועד לעיבוד ממוחשב, למעט: אוסף לשימוש אישי שאינו למטרות עסק. אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני אדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף.
	5. **משתמש -** כל מי שעושה שימוש חוקי במערכות המידע.
	6. **מנהל מערכת -** מנהל שבתחום אחריותו מערכת מידע והיחידה שבניהולו היא המשתמש הראשי במערכת.
	7. **משתמש אדמיניסטרטיבי -**  משתמש בכיר או ראשי במערכת מסוימת, לרוב בעל הרשאות תפעוליות גבוהות.
	8. **מנהל מאגר מידע -**  מי שהאוניברסיטה הסמיכה אותו כמנהל מאגר מידע של מאגר מידע אחד או יותר.
	9. **מערכת ליבה –**מערכת מידע תפעולית מרכזית ומשמעותית עבור פעילות האוניברסיטה. ככלל הכוונה למערכת חיונית לפעילות היומיומית השוטפת של האוניברסיטה, או שמתבצעת בה פעילות בעלת חשיבות רבה לאוניברסיטה, ושיש בה נפח פעילות ומשתמשים משמעותי או כאלה המכילה נתונים בעלי רגישות מיוחדת.
	10. **משתמש חיצוני** **-** כל ספק, יועץ חיצוני, נותן שירותים לאוניברסיטה או כל גורם אחר שאינו

סטודנט באוניברסיטה ואינו עובד של האוניברסיטה והנדרש להשתמש במערכות המידע שלה

 לצורך ביצוע תפקידו.

* 1. **גישה מרחוק (Remote Access) -** חיבור מרחוק של משתמש, לרבות משתמש חיצוני מחוץ רשת

 האוניברסיטה אל המערכות של האוניברסיטה.

* 1. **בקרה מפצה-** תהליך או טכנולוגיה חלופית הנועדה להפחית את הסיכון איתו האוניברסיטה

 מתמודדת.

* 1. **רשת האוניברסיטה -** מערכת המיועדת לתקשורת בין מספר מחשבים- רשת המנוהלת ע"י

 מחלקת תשתיותIT של האוניברסיטה.

* 1. **רשת יחידתית -** מערכת המיועדת לתקשורת בין מספר מחשבים- ומנוהלת ע"י איש המחשוב ביחידה

 האוניברסיטאית.

* 1. **עקרון הצורך לדעת(Need to know)** - עיקרון מבוסס על הקונספט של מתן הרשאות גישה רק למידע

 הנדרש לביצוע התפקיד.

1. **תוכן הנוהל**
	1. **מדיניות הרשאות כללית:**
		1. הקצאת ההרשאות תהינה ע"פ דרישה ועל בסיס התפקיד (Role Base Access Control)..
		2. ההרשאות תפוצלנה בהתאם לצורך בין בעלי תפקידביצועי, מאשרי הרשאות - מנהלי מערכות

 ומשתמשים אדמינסטרטיבים, גם באותו תחום.

* + 1. ההרשאות תפוצלנה בין תפקידי מפתח במערכות, בהתאם להגדרות מנהל המאגר ו/או מנהל

 אבטחת מידע. ( מפוצלות או תפוצלנה, בהמשך לנוהל).

* + 1. בקרות מפצות יקבעו על ידי מנהלי המערכת ומנהל אבטחת המידע, במקרים בהם קיימת חריגה

 מעקרון הפרדת סמכויות מנהל המערכת יבצע בחינה תקופתית על יישום הבקרות.

* + 1. מנהל המאגר ומנהל אבטחת מידע יקצו הרשאות בתחומים שיוגדרו כרגישים על ידם

 בתאום הממונה על מנהל המאגר האחראי על התחום בו ניתנות ההרשאות.

* + 1. הגדרת רמות מידור והרשאות: למשתמשים שהינם עובדים באגף והנדרשים להרשאות חזקות

 דוגמת Domain Admin מוקצים שני חשבונות משתמש:

1. **חשבון משתמש בעל הרשאות רגילות** בו ישתמשו במהלך עבודתם השוטפת באוניברסיטה;
2. **חשבון בעל הרשאות חזקות** ואשר בהן ייעשה שימוש רק בהתאם לצורך אדמינסטרטיבי.
	* 1. עבודה בתחנות קצה - מבוצעות ע"י חשבון רשתי עם הרשאות משתמש מוגבלות.
		2. חשבונות ברירת המחדל ינוטרלו.
		3. התחברות ליישומים ואימות על ראשי (Single Sign On) המשמש לכניסה לרשת- ככל האפשר.

 גישה למאגרי מידע יבוצעו ע"ב 2FA (הזדהות באמצעות שני גורמים).

* + 1. מימוש כלל הסעיפים הנ"ל בכפוף למגבלות טכנולוגיות של המערכת.
	1. **דרישות להקמת משתמש חדש**
		1. הקמת משתמש חדש תתאפשר רק למשתמשים שהסתיים עבורם תהליך הקליטה

 לאוניברסיטה ולאחר חתימת כל הגורמים הנדרשים.

* + 1. מנהל היחידה יפנה דרישה למחלקת IT באמצעות טופס הטיולים למתן מחשב וגישה למערכות

 המידע עבור עובד חדש או קבלן חדש.

 הדרישה חייבת לכלול מספר עובד או מספר קבלן ותיאור תפקיד ורמת ההרשאה הנדרשת.

* + 1. "המחלקה " תעביר לעובד פרטי המשתמש והסיסמה -בכניסה ראשונית למערכות

 האוניברסיטה יחויב העובד להחליף את הסיסמאות שניתנו לו.

* + 1. העובד יחתום על הטפסים הרלוונטיים המצוינים בנוהל אבטחת מידע במשאבי אנוש.
		 הרשאות ניהול של שרתים ומערכות תקשורת ברשת יינתנו ע"פ הנחיה של מנהל IT.
		2. הרשאות למערכות אבטחה יינתנו ע"פ הנחיה של מנהל אבטחת מידע.
		3. לכל מחלקה באוניברסיטה יהיה פרופיל הרשאות ייעודי- מתן הרשאות למשתמש חדש יתבסס

 ככל שניתן על סט הרשאות קיים למשתמש בתפקיד דומה.

* + 1. כל משתמש חיצוני המבקש לקבל הרשאה לחיבור קבוע יאושר רק בכפוף להסדרת

 התחייבויותיו באמצעות חוזה בכתב.

* + 1. ככל שניתנת הרשאה למאגר מידע, יש לפעול בנוסף בהתאם להוראות נוהל ניהול מאגרי מידע.
	1. **עדכון הרשאות לחשבון משתמש קיים:**
		1. משתמש שנדרש במסגרת תפקידו להרשאות נוספות מעבר להרשאות הקיימות, לרבות לצורך

 מתן גישה למערכות נוספות, יפנה בבקשה לממונה הישיר שלו ויפרט את הסיבה לבקשה.

* + 1. ככל והממונה הישיר אינו מנהל המערכת או מנהל מאגר מידע, הממונה הישיר יעביר את

 הבקשה לאישור מנהל המערכת או מנהל מאגר המידע, לפי העניין.

* + 1. בקשה שאושרה תועבר לביצוע לרישום אצל מנהל המערכת ולמנהל אבטחת המידע באגף

 טכנולוגיות ודיגיטל שיהיה אחראי לעדכן את ההרשאות בהתאם לבקשה שאושרה.

* + 1. **עדכון הרשאות בעת מעבר תפקיד:** בכל מעבר תפקיד של משתמש באחריות הממונה הישיר

 הקודם לוודא מול מנהלי המערכות הרלוונטיים שהוסרו ההרשאות שלא נדרשות למשתמש

 בתפקידו החדש.

* 1. **סיום העסקה**
		1. במקרה של סיום העסקה יועבר למחלקת ה-IT, ע"י מנהל מחלקה, הודעה עם ההרשאות

 הנדרשות להסרה.

* + 1. במקרים חריגים(כגון פיטורים) בהם קיים חשש כי יבוצעו פעולות לפגיעה במידע הארגוני מנהל

 האבטחת מידע נדרש להסיר הרשאות במידית ולבצע ניטור לזיהוי חריגות בפעילות העובד.

* + 1. **מחלקת IT אחראית לוודא במקרה של סיום העסקה:**
			- 1. ביטול הגדרות משתמש ברשת.
				2. סגירת העובד במערכות העסקיות.
	1. **תהליך טיפול בהרשאות במקרים חריגים**
		1. במקרה של קבלת עובד חדש ורצון לשמר את הפרופיל של העובד שעוזב, מנהל המחלקה נדרש

 לשלוח דוא"ל למנהל אבטחת מידע ביחד עם הדרישה.

* + 1. במידה ומנהל אבטחת מידע יאשר את הבקשה- יחידת ה-IT תשמר את הפרופיל אך תשנה את

 שם המשתמש וסיסמה של העובד העוזב.

* 1. **מעקב וביקורות:**
		1. האגף ירכז רשימה של מערכות המידע בתחומו כולל הנחיות ספציפיות לגבי מתן הרשאות גישה

 ככל שיוגדרו על ידי מנהל המערכת. הרשימה תעודכן מעת לעת בהתאם לשינויים ו/או בקרה

 תקופתית של האגף .

* + 1. רפרנטי מחשוב בפקולטות ירכזו רשימה של מערכות המידע בתחומן כולל הנחיות ספציפיות

 לגבי מתן הרשאות גישה ככל שיוגדרו על ידי מנהל המערכת. הרשימה תעודכן מעת לעת

 בהתאם לשינויים ו/או בקרה תקופתית של האגף.

* + 1. **מנהל אבטחת מידע יבצע ביקורות עיתיות, ויעדכן במידת הצורך, את הרשאות המשתמשים**

 **במערכות, בתיאום עם מנהל המערכת הרלוונטי. הביקורת תכלול:**

1. בחינת רשימת משתמשים בעלי הרשאות גבוהות.
2. ביצוע ניסיון יזום לגישה באמצעות חשבונות של עובדים שעזבו, בדגש על עובדים שהיו להם חשבונות ניהול וחשבונות עם הרשאות לפעולות משמעותיות.
3. בדיקה מדגמית של חשבונות לבחינת עודף הרשאות.
4. ניסיון גישה לרכיבים/קבצים/שירותים אשר לא הוגדרו לחשבון. ייבחן אם נרשם בלוג ב-SIEM וקופצת התרעה ב-SOC.
	1. **סקר ובקרת הרשאות**
		* 1. באחריות מנהל המערכת לבצע **אחת לשנה לכל הפחות,** בקרה על ההרשאות למערכות השונות. במסגרת זו יבחן מנהל המערכת את ההרשאות הקיימות ויוודא כי היקף ההרשאות לא חורג מעבר לנדרש לצורך מילוי תפקידו של כל משתמש. ככל שהתגלו חריגות או הרשאות שיש לבטלן, מנהל המערכת יסיר או יגביל את אותן הרשאות חורגות.
			2. באחריות מנהל המאגר לבצע אחת לשנה לכל הפחות, בקרה על ההרשאות למערכות השונות. במסגרת זו יבחן מנהל המערכת את ההרשאות הקיימות ויוודא כי היקף ההרשאות לא חורג מעבר לנדרש לצורך מילוי תפקידו של כל המשתמש. ככל שהתגלו חריגות או הרשאות שיש לבטלן, מנהל המערכת יסיר או יגביל את אותן הרשאות חורגות.
			3. בתום השלמת הבקרה לעיל, מנהל מערכת יעביר למנהל אבטחת מידע דו"ח המפרט את השינויים בהרשאות.
5. **אחריות לביצוע:**
6. **אגף טכנולוגיות חדשנות ודיגיטל** – אחראי לקיום ולעדכון הנוהל וכן התפעול והבקרה של השימוש במשאבי המחשוב.
7. **הועדה לאבטחת מידע** – מופקדת על התווית המדיניות בסוגיות הנוגעות לנוהל זה, בתאום עם הועדה למדיניות המחשוב (ראו הפניה).
8. **המשתמש עצמו** – ינהג על פי הכללים, הנהלים והאתיקה של האוניברסיטה המתפרסמים מעת לעת ע"י אגף טכנולוגיות חדשנות ודיגיטל ובכפוף לחוק הגנת הפרטיות .(ראו הפניה)

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