1. כללי

תפעול יעיל ומעקב אחר אירועים ברכיבי אבטחת המידע הנה פעילות נדרשת לצורך זיהוי אירועי אבטחת מידע ומתן מענה מהיר ואפקטיבי. ביצוע פעולות מעקב שוטפות תעלה את רמת אבטחת המידע במכללה האקדמית.

1. מטרה
2. קביעת סדרי תיעוד, ניטור ובקרה על מערך רכיבי אבטחת המידע במכללה.
3. לשמור על שלמות וזמינות מערכות אבטחת המידע ולאתר כשלים ופעילויות לא מורשות.
4. הגדרת מושגים

|  |  |
| --- | --- |
| המכללה | המכללה האקדמית של תל אביב יפו |
| מרכז תמיכה | מרכז תמיכת המחשוב של המכללה  |
| גורמים מטפלים | כל אותם הגורמים שמעורבים בטיפול בפנייה ובעלי גישה למערכת הפניות. |
| CA Service Desk | מערכת הפניות CA Service Desk המשמשת את מרכז התמיכה והגורמים המטפלים לתפעול ותיעוד הפניות. |
| בקשת שינוי | כל בקשה לשינוי או מתן הרשאות גישה לרכיב מחשוב, רשת, קובץ, אתר אינטרנט או אחר. |
| משתמש | משתמש בשירותי המחשוב של המכללה המוגדר חד ערכית במערכות המחשוב של המכללה, לרבות משתמשים המתחברים מבחוץ לרשת המכללה. |
| גורם מאשר | הגורם המאשר את בקשות השינוי לפני ביצוע שינוי בפועל . |
|  |  |

1. אחריות

האחריות לעבודה על פי הנוהל חלה על הגורמים הבאים:

* + - * מנמ"ר המכללה
			* מנהל האתר
			* מנהלי רשת המחשבים במכללה
			* כל גורם מאושר אחר
1. שיטה
	1. המערכות

במכללה מותקנים רכיבי אבטחת המידע הבאים:

1. **Firewall של חברת Juniper בגרסא SSG550M -** מערך Firewall של המכללה הנו רכיב אבטחת המידע העיקרי המאפשר ניהול תעבורת רשת על פי מדיניות מוגדרת וחוצץ בין רשת הפנים משרדית לרשתות חיצוניות לרבות מבח"ר, אינטרנט, חברת NESS וקישור מרוחק. המערכת משמשת כחוצץ בין הרשת של המכללה לרשתות חיצוניות .
2. **מערכת SSL VPN של חברת Juniper מסוג Mag2600 –** מערכת קישור משתמשים חיצוניים לרשת המכללה. המערכת משמשת להתחברות לעבודה מרוחקת עבור משתמשי המכללה ,ספקים חיצוניים ומאגרי ספרייה מרחוק ,וכן לצרכי ניהול, תפעול שוטף ותחזוקת מערכות.
3. **מערכת אנטיוירוס (AV) של חברת Microsoft מסוג System Center Endpoint Protection –** המערכת משמשת לסריקת וירוסים ומנוהלת ע"י מערכת SCCM .
4. **מערכת Web Application Firewall** של חברת **Imperva** - חומת אש אפליקטיבית שנועדה להגן על אתרי האינטרנט השונים של המכללה.
5. **שרת Proxy של חברת Microsoft מסוג** **Threat Management Gateway** – תוכנה המותקנת על שרת ונועדה לסינון אתרים (פורנו, שיתוף קבצים וכו') וחסימת URL’s ופרוטוקולים שונים.

* 1. עקרונות ניטור ותיעוד במכללה
1. תיעוד לוגים ממערכות אבטחת המידע מבוצע באופן שוטף ומלא.
2. מערכות אבטחת המידע במכללה שומרות לוגים גם באופן מקומי וגם שולחות מייל התרעה.
3. הלוגים שישמרו ישמשו לצורך ניתוח אירועי אבטחת מידע שיזוהו בפועל ולא כבקרה שוטפת.
4. כל מייל התרעה שנשלח ממערכת אבטחת מידע ינותח ויתוחקר ONLINE.
5. ספק האינטרנט של המכללה מתריע על אירועי אבטחת מידע חריגים שזוהו בפועל וטופלו על ידם.
	1. הגדרת אירועים לבקרה
		1. מערכת Firewall
6. שינוי בהגדרות המערכת.
7. שינוי בהרשאות משתמש.
8. שינויים שנעשו על ידי משתמשים מורשים
9. ניסיונות גישה כושלים לניהול המערכת.
10. הוספה/הסרה של חשבון משתמש ניהולי.
11. ניסיונות לסריקת פורטים
12. התנהגות רשת חריגה ( Flood )
	* 1. מערכת SSLVPN
13. שינוי בהגדרות המערכת.
14. שינוי בהרשאות משתמש.
15. שינויים שנעשו על ידי משתמשים מורשים
16. ניסיונות גישה כושלים לניהול המערכת.
17. הוספה/הסרה של חשבון משתמש ניהולי.
	* 1. מערכת אנטי וירוס
18. חדירה של וירוס לתחנת קצה
19. ביצוע עדכונים אוטומטיים בתחנת קצה
20. חוסר בעדכוני חתימות וירוסים בשרת
	* 1. WAF – Imperva

א. שינוי בהגדרות המערכת.

ב. שינוי בהרשאות משתמש.

ג. שינויים שנעשו על ידי משתמשים מורשים

ד. ניסיונות גישה כושלים לניהול המערכת.

ה. הוספה/הסרה של חשבון משתמש ניהולי.

1. חסימת גישה זדונית לאתר.
	* 1. Proxy – TMG
2. ניסיון משתמשים לגישה לאתרים אסורים
3. מקסימום חיבורים ממקור אחד לדקה
	1. טיפול באירועים

הטיפול באירועים במערכות אבטחת המידע יעשה בהתאם למפורט להלן:

* + 1. מערכת Firewall
1. מיד בקבלת התרעה על אירוע הנחשד כתקיפה תתקבל התרעה במייל למנהלי הרשת , תבוצע חקירת אירוע וטיפול על ידי מנהל רשת המחשבים . במידה והאירוע גורם לחסימת שירותים\איטיות\הפלת אתרים יש לדווח מיידית למנמ"ר המכללה.
2. שינויים שבוצעו ללא אישורים מתאימים ונמצאו כבלתי רצויים יוסרו.
3. יערך בירור עם הגורמים המעורבים לצורך הבהרת התהליך התקין.
	* 1. מערכת SSL-VPN
4. מיד בקבלת התרעה תבוצע חקירת אירוע וטיפול על ידי מנהל רשת המחשבים.
5. שינויים שבוצעו ללא אישורים מתאימים ונמצאו כבלתי רצויים יוסרו.
6. יערך בירור עם הגורמים המעורבים לצורך הבהרת התהליך התקין.
	* 1. מערכת אנטי וירוס
7. בקבלת אירוע על חדירת וירוס תסרק התחנה שנית על מנת לוודא שההתרעה אינה חוזרת על עצמה. התרעה במייל נשלחת למנהלי הרשת. מיד בקבלת התרעה זו , מנהלי הרשת בודקים את חומרת האירוע ומדווחים למנמ"ר המכללה אם מדובר באירוע חריג
8. מיד בקבלת התרעה על חוסר בעדכוני חתימות וירוסים בתחנת הקצה יבוצע עדכון ידני להורדת חתימות חדשות מהשרת.
9. מיד בקבלת התרעה על חוסר בעדכון חתימות וירוסים בשרת תבוצע הורדה ידנית של חתימות.
	* 1. מערכת IMPERVA
10. מיד בקבלת התרעה על אירוע הנחשד כתקיפה תבוצע חקירת אירוע וטיפול על ידי מנהל רשת המחשבים.
11. שינויים שבוצעו ללא אישורים מתאימים ונמצאו כבלתי רצויים יוסרו.
12. יערך בירור עם הגורמים המעורבים לצורך הבהרת התהליך התקין.
	* 1. מערכת TMG
13. בעת גילוי ניסיון גישה לאתר חסום המשתמש יקבל הודעת שגיאה המודיעה על החסימה
14. בעת גילוי ניסיון תקיפה ע"י מסבר רב של חיבורים המשתמש יקבל הודעת שגיאה המודיעה על החסימה.
	1. תיעוד ומעקב
15. אחת לחודש מופק דוח אירועים חריגים.
16. דוח אירועים מכיל תאריכי פתיחה וסגירה של האירוע ואופן הטיפול.
17. הדוחות חתומים על ידי מנהל רשת המחשבים ומהל האתר ומועברים למנמ"ר המכללה.
18. רשימת השינויים

| תאריך | מהדורה | תיאור השינוי | גורם מבצע |
| --- | --- | --- | --- |
| 12/5/15 | 1.0 | כתיבת נוהל ניטור ובקרה ברכיבי אבטחת מידע  | ליאור כהן |