מערכות מידע - אבטחת מידע		**מספר:**	27-000-18
		סטאטוס:	
תחום:	27	ניהול אבטחת מידע	**מהדורה:** 1.2
נושא:	000	הגנת הפרטיות	**תאריך מהדורה:** 7/11/2018
נוהל:	18	**נוהל ניהול מאגרי מידע – הגנת פרטיות**	עמוד 1 מתוך 11

מתייחס לתקן: ISO27001:2013 ולתקנות הגנת הפרטיות 2017

מסמכים ישימים:

1. **נוהל ניהול אירוע סייבר - 27-000-03**
2. **נוהל ניהול משתמשים - מערכות מידע 27-000-08**
3. **מסמך מדיניות מלם-תים (Data Security Policies) ע"פ הנחיות תקן ISO27001:2013**
4. **נוהל אסקלציה – הגנת הפרטיות במאגרי מידע 27-000-19**

נספחים:

5. **נספח א' - תבנית מסמך הגדרות המאגר - בעל המאגר**
6. **נספח ב' - תבנית מסמך הגדרות המאגר – מחזיק המאגר**
7. **נספח ג' - כתב מינוי מנהל מאגר במוסט**
8. **נספח ד' – רשימת תיוג (check list) לתיקוף שנתי למסמכי הגדרת המאגר**
9. **נספח ה' – טופס תיעוד טכנולוגי – מבנה המאגר**

הסטורית שינויים

גירסה/ עדכון מס'	תאריך	מעדכן	תאור השינוי / סיבת השינוי
0.1	7/5/2018	אלי שפרון	נוהל חדש – בעקבות תקנות הגנת הפרטיות החדשות (אבטחת מידע), תשע"ז-2017
1.1	22/8/2018	אלי שפרון	עדכון חובת הודעה על אירוע והחלפת נספח א' בעקבות שינויי עריכה קלים בטופס
1.2	7/12/2018	אלי שפרון	שינויים קלים להתאמה לתקנות בעקבות הערות ועדת ההיגוי והוספת נספח – טופס תיעוד טכנולוגי
1.3	7/8/2019	אלי שפרון	הוספת התייחסות להקמת אגר חדש והצורך לבדוק נחיצות מידע אישי רגיש במאגר

אישורים

גירסה/ עדכון מס'	תאריך	פעולה	מבצע – תפקיד
0.1	28/5/2018	עריכה	אלי שפרון – מנהל האיכות
1.0	30/6/2018	אישור	ועדת היגוי הגנת הפרטיות
1.2	19/12/2018	אישור	ועדת היגוי הגנת הפרטיות
1.3	7/8/2019	אישור	ועדת היגוי הגנת הפרטיות

0. כללי :

מוסט משקיעה משאבים רבים לשמירה על הזכות לפרטיות של האנשים שמידע אודותיהם אגור במאגרי המידע שבבעלות החברה או במאגרי מידע המוחזקים על ידה.

החברה מפעילה אמצעים למניעת שימוש במידע שלא למטרה שלשמה הוא נאסף מתוך הכרה שהזכות לפרטיות היא נדבך חשוב בזכויות האדם והפרט ומתוך ציות לדרישות חוק הגנת הפרטיות.

הגנת הפרטיות היא חלק ממערך אבטחת המידע בחברה.

1. מטרה

הגדרת שיטה אפקטיבית לשמירה על פרטיות המידע והנחיית בעלי התפקידים הרלוונטים בחברה ביישום דרישות חוק הגנת הפרטיות העדכני בכל הנוגע להחזקה ושימוש במאגרי מידע.

2. הגדרות:

מאגר מידע	אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב למעט אוסף לשימוש אישי שאינו למטרות עסק.
בעל מאגר מידע / בעל המאגר	**הארגון** שמאגר המידע שייך לו
משתמש במאגר מידע	מי שעושה שימוש (עדכון, שינוי, הוספה, העתקה, מסירה, העברה) במידע שבמאגר המידע
מידע אישי רגיש	כהגדרתו בחוק הגנת הפרטיות, ובאופן כללי: נתונים הנוגעים לצנעת הפרט, כגון מצבו הבריאותי של אדם, מצבו הכלכלי, דעותיו ואמונתו
נושא המידע	האדם שעל אודותיו קיים מידע במאגר המידע
מנהל המאגר	מנהל פעיל במוסט או מי שהוסמך על ידו לניהול מאגר שבבעלות החברה או בהחזקתה.
מחזיק המאגר	מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי (ברשות בעל המאגר) לעשות בו שימוש
ממונה הגנת מידע של המאגר	עובד שכפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, או לנושא משרה בכירה אחרת הכפוף ישירות למנהל המאגר.
גורם חיצוני מורשה	גורם חיצוני שקיבל הרשאה מבעל המאגר או ממחזיק המאגר לעשות שימוש במאגר.
מסמך הגדרות המאגר	מסמך הנדרש על פי חוק מבעל המאגר ובו מידע אודות המאגר תבנית (template): ראה נספח א ונספח ב'
מסמך מלווה למאגר	מסמך עזר של מוסט ובו מידע אודות המאגר בו מחזיקה החברה כ"גורם חיצוני" לבעל המאגר (מסמך וולנטרי) תבנית (template): ראה נספח ב'
מדיניות מלם-תים	מדיניות אבטחת המידע של מלם-תים (Data Security Policies) ב 18 תחומים של אבטחת מידע - ע"פ הנחיות תקן ISO27001:2013 כפי שהיא מתועדת במסמך המדיניות בפורטל הארגוני.

3. תחולה

נוהל זה חל על מאגרי מידע המכילים מידע אישי רגיש ברמת האבטחה שבהם מוסט הינה בעל המאגר או גורם חיצוני מחזיק המאגר עבור אחרים.

במקרים שבהם מוסט מוגדרת כ"מחזיק המאגר" או כ"גורם חיצוני" חובתו של בעל המאגר להנחות אותה באופן יישום החובות בתחום אבטחת המידע לפי תקנות הגנת הפרטיות, ובמידת הצורך להציב הנחיות נוספות לעניין אמצעי אבטחת מידע. בהעדר הנחיות, ישמש הכתוב ב"מסמך הנחיות המאגר" (נספח ב') כהנחיה למורשי הגישה לצורך הגנה על המידע.

4. שיטה

שיטת אבטחת המידע וההגנה על מידע אישי מיישמת מספר רבדים של הגנת המידע:

- **ניטור ומניעת פגיעה פיזית** במערכות המידע (שמירה, הגבלות גישה, הגנה בפני נזקי חשמל מים, אש וכיו"ב)
- **ניטור והגבלות גישה למערכות המידע** (סיסמאות, תוכנות הגנה)
- **פעולות למודעות עובדים** ולהנחיתם בנגע לשימוש ולגישה למאגר

4.1 <u>הגישה למערכות המידע</u>

4.1.1 הרשאות

הרשאות לגישה לנתוני מאגר יינתנו רק באישור מנהל המאגר או באישור מי שהוסמך על ידו להקצות הרשאות גישה למאגר.

בעת הקצאת הרשאה חדשה ובעת הרחבת הרשאה קיימת למאגר ובו נתונים אישיים רגישים, באחריות מנהל המאגר לברר:

א. שאין חשש כי מקבל ההרשאה אינו מתאים לקבלת גישה למידע אישי רגיש המצוי במאגר;

ב. שמקבל ההשאה אכן צריך את הגישה לצרכי עבודתו ותפקידו.

הגישה למידע במאגר תהיה רק למורשים לגישה **למאגר הספציפי** ובהתאם להנחיות השימוש שקיבלו (ראה נספח ב')

בעלי הרשאות גישה יחשפו למידע בהתאם לתחום עיסוקם ויתאפשר להם לבצע פעולות בהתאם לרמת ההרשאה שקיבלו.

הנחיות בנושא ניהול הרשאות וסיסמאות הגישה לנכסי המידע בחברה, ראה: נוהל ניהול משתמשים מערכות מידע 27-000-08

4.1.2 בקרות על הגישה למאגר / תיעוד הגישה למאגר

הגישה למאגר תבוקר באמצעות תוכנות בקרה המתעדות גישה למאגר.

לפחות אחת לשנה, אך גם בעקבות שינויים (כגון פרישת עובד מורשה) או בעקבות אירוע אבטחת מידע, באחריות מנהל המאגר לתקף את רשימת המורשים ולבדוק האם ההרשאות הקיימות עדיין רלוונטיות לתפקידם (למשל, האם כל מי שמוגדר כבעל הרשאה אכן עדיין עובד בחברה בתפקיד המצריך גישה למאגר). מנהל אבטחת המידע של המאגר יבדוק שהקצאת ההרשאות במערכת ניהול ההרשאות אכן מבטאת את הנדרש ע"י מנהל המאגר. כמו כן יבדוק האם נעשו ניסיונות גישה למאגר ע"י מי שאינם מורשים, או ניסיונות גישה של מורשים למידע או פעולות שהם אינם מורשים להם.

בעקבות ממצאי הבקרה יורה על ביצוע שינויים ובמידת הצורך פעולות מתקנות, ואם נדרש, יפעל לנקיטת צעדים משמעתיים.

4.1.3 אמצעי אבטחה, זיהוי ואימות למערכות המאגר

באחריות אגף מערכות המידע להתקין ולתחזק מערכות הגנה על הנתונים והתקשורת ולתחזק מנגנון תיעוד שיאפשר:

א. בקרה על הגישה למערכות המאגר,

ב. ביצוע בקרות תקופתיות ,

ג. תחקורים

ד. שמירת המידע הנאסף לתקופה של שנתיים לפחות.

4.1.4 הנחיות למורשי הגישה למאגר - הגנה על המידע

עובדי החברה בכלל, ומורשי הגישה למאגרים שיש בהם מידע אישי רגיש ברמת האבטחה הבינונית והגבוהה בפרט, יקבלו הנחיות מפורטות ממנהל המאגר בדבר המותר והאסור בשימוש במאגר (ראה מסמך ההנחיות בנספח ב') בדגש על כך שאין להשתמש במידע שבמאגר שלא למטרה שלשמה הוא נאסף מלכתחילה

4.1.5 מינוי מנהלי מאגר

מנכ"ל החברה הוא האחראי למילוי החובות שמוטלות בחוק על מנהל המאגר. לכל מאגר מידע שיש בו מידע אישי רגיש והוא בבעלות החברה, ימנה מנכ"ל החברה מנהל מאגר מתאים שיהיה עובד בכיר בחברה שעבר בהצלחה תהליכי קליטה ומיון בחברה ושביכולתו לפעול באופן עצמאי על מנת לקיים את חובותיו כמנהל המאגר על פי חוק. המינוי יתועד ב"כתב מינוי" (נספח ג') ומנהל המאגר יאשר את קבלת המינוי.

- כאשר ה Data Center הוא מחזיק המידע במאגר - אין למנות מנהל מאגר שהוא בעל תפקיד ב Data Center.
- ממונה אבטחת מידע וכל מי שיש ניגוד עניינים בין תפקידו לבין המידע שבמאגר לא ימונה כמנהל מאגר.

מסמך הגדרות המאגר

באחריות מנהל המאגר לתעד את מטרות איסוף המידע, נתוני מורשי גישה ונתונים נוספים ב"מסמך הגדרות המאגר" (נספח א'). מנהל אבטחת המידע של המאגר יחליט על סמך הנתונים הקיימים והצפויים ובהתאם להנחיות החוק, על רמת האבטחה הנדרשת ויתעד זאת בחתימתו בטופס.

לאחר המילוי, באחריות מנהל המאגר לשמור את המסמך, לתקף אותו אחת לשנה.

בקרת התיקוף תכלול:

- שינויים משמעותיים הקשורים להגדרות המאגר (טכנולוגים, ארגוניים, שינויי תוכן)
- בקרה האם המאגר היה מעורב באירוע אבטחה
- האם מוחזק במאגר מידע רב מהדרוש על פי המטרות
- האם חלו שינויים בבעלי הגישה (האם כולם רלוונטים)

- האם ישנם סיכונים חדשים

מנהל המאגר יעדכן את המסמך בהתאם לממצאי התיקוף ויפעל להפחתה סילוק של סיכונים שהתגלו

ראה נספח ד׳

4.1.6 הנחיות כלליות

- <u>הדרכת מורשים</u>: באחריות מנהל המאגר להדריך כל עובד שיקבל הרשאת גישה למאגרי מידע שבבעלות החברה ובהם מידע אישי רגיש. ההדרכה תכלול הנחיות לשימוש במידע בהתאם לרמת ההרשאה שתינתן לעובד (ראה גם סעיף הדרכה)
- <u>הרשאות גישה</u>: הקצאת הרשאת גישה למשתמש בעל הרשאה רחבה (כגון admin) תהיה באישור מנהל המאגר או מי שהוסמך מטעמו ורק לאחר שווידא שאכן יש בכך צורך. הרשאה זו תתועד באחריות מנהל המאגר / נותן ההרשאה. ככלל – יש למעט בבעלי הרשאת admin
- <u>גישות זמניות</u>: גישה שנפתחה לצורך תמיכה או תחזוקה (למשל: השתלטות מרחוק) תיסגר מיד בתום השירות – באחריות מזמין השרות לוודא ניתוק.
- <u>פתיחת נעילת הרשאה</u>: פתיחת משתמש שננעל (לאחר מספר מוגדר של ניסיונות כושלים לגישה למערכת) תהיה רק לאחר בירור סיבת הנעילה ואימות זהות המשתמש וזכויות הגישה למאגר אליו ביקש להיכנס.
- <u>העברת מידע</u>: העברת מידע רגיש מחוץ למתקני החברה תהיה בהתאם למוגדר במסמך הגדרות המאגר ו/או הנחיות בעל המאגר ובהתאם ל ״מדיניות העברת מידע״ שבמסמך מדיניות מלם תים
- הקמת מאגר חדש: לפני הקמת מאגר חדש ובו מידע אישי רגיש חובה לבדוק האם יש צורך אמיתי בשמירת המידע האישי במאגר והאם רק מידע אישי הכרחי לפעילות שלשמה מוקם המאגר, יישמר במאגר. על מקים המאגר לדווח לממונה אבטחת המידע בחברה על המאגר החדש ולקבל הנחיותיו לעמידה בדרישות החוק והחברה.

4.1.7 סיכונים למידע והטיפול בהם

באחריות מנהל המאגר לנהל סיכונים בהקשר למאגר. תיעוד המעיד על ביצוע תהליך ניהול סיכונים ישמר אצל המנהל האחראי על הגנת הפרטיות. באחריות מנהל המאגר לנהל את הסיכונים למאגר ולתעד זאת ב״מסמך הגדרות המאגר – בעל המאגר״

כאשר הסיכונים מנוהלים ברמה הארגונית או למספר מאגרים ביחד, מסמך הגדרות המאגר יפנה או יצביע על מסמך הסיכונים הכללי.

4.1.8 גיבוי ושיחזור נתוני המאגר

באחריות מנהל המאגר או מי שהוסמך מטעמו, למסור הנחיות גיבוי לצוות מערכות המידע/ Data Center, ולוודא כי נתוני מאגר המידע מגובים תקופתית בהתאם לנהלי הגיבוי וניתנים לאיחזור במקרה הצורך.

אחת לתקופה המוגדרת בנוהל או בהנחיות בעל המאגר, יבוצע שיחזור יזום ויתועד ע״י מבצעי השיחזור.

פעולות איחזור שבוצעו במהלך התחזוקה השוטפת - יתועדו ע״י מחזיק המאגר.

ראה גם: נוהל גיבוי ושחזור מערכות מידע 27-000-07

4.1.9 התמודדות עם אירועי אבטחת מידע

בכל אירוע של פגיעה או חשש לפגיעה, בשלמות וסודיות נתוני **מידע אישי רגיש** המצויים במאגרי מידע שבבעלות החברה או באחזקתה, ידווח מזהה הפגיעה או מקבל ההתרעה לממונה הישיר - במקביל לטיפול בצד הטכני של מניעה/התמודדות, יפנה לממונה הגנת הפרטיות בחברה להחלטה, לאחר התייעצות עם המחלקה המשפטית, האם נדרש דיווח לבעל המאגר, לנושאי המידע או לאחרים (הנחיות מפורטות, ראה: נוהל אסקלציה – הגנת הפרטיות)

בעת התראה על אירוע סייבר או בעת האירוע עצמו יופעל "סדר פעולות ליישום באירוע סייבר" המצוי בחוות השרתים וביחידת מערכות המידע – על פי נוהל ניהול אירוע אבטחת מידע וסייבר

4.1.10 הנחיות שימוש בהתקנים ניידים בסביבות המאגר

שימוש בהתקנים ניידים בסביבת מאגרי מידע הכוללים מידע אישי רגיש ברמת אבטחה בינונית ומעלה, יהיה בהתאם להנחיות מדיניות מלם-תים בנושא – ראה: מסמך מדיניות מערכת ניהול אבטחת מידע – סעיף 14 מדיניות שימוש ברכיבים חיצוניים ופרטיים (BYOD)

4.1.11 בקרות תקופתיות לאימות ותקפות אמצעי האבטחה

אחת לשנה לפחות ייערכו בקרות מדגמיות לבחינת אפקטיביות אמצעי האבטחה בהתאם לתכנית ניהול אבטחת המידע בחברה. ההכשרה והניסיון הנדרשים לביצוע הבקרות בנושאים אלו יהיו בהתאמה לרגישות המידע ולמורכבות המערכות באופן שיאפשר לבודק לבצע את תפקידו, לבחון נהלים, להעריך סיכונים, לזהות ליקויים, ולהציע אמצעים לתיקונם.

הבקרה תיערך באמצעות אחת או יותר מהפעילויות הבאות:

- מבדק פנימי (Audit) לבקרת יישום בפועל של הנחיות הנהלים ולבחינת התהליכים,
- בקרות ע"פ SOC,
- סקר סיכונים,
- מבדקי חדירה,
- בדיקת Logs וכיו"ב.

באחריות מנהל המאגר לוודא שהמאגר שבניהולו אכן נבדק.

ראה גם: נספח ד' –לתיעוד התיקוף השנתי של מסמך הגדרות המאגר.

4.1.12 מאגרי מידע של לקוח במהלך פיתוח ותחזוקה של מערכות מידע

בפיתוח ובתחזוקה של מערכות מידע עבור לקוחות החברה, סביבות העבודה של הפיתוח, הבדיקות ההסבה וטיוב הנתונים המצויות בחברה לא יכילו מאגר ובו נתוני אמת של מידע אישי רגיש.

באחריות מנהל הפעילות/הפרויקט לקבל הנחיות ואישור בכתב מבעל המאגר לשיטה מוסכמת לצורת שמירת/תצוגת מידע אישי רגיש במחשבי מוסט (ערבול מידע, הצפנה, או כל שיטה מקובלת אחרת למניעת זיהוי נושאי המידע במאגר) בהיעדר אישור כזה – חל איסור להחזיק מאגר אישי רגיש במחשבי החברה.

במקרים שבעל המאגר מעביר למחשבי החברה העתק מאגר לצורך בדיקות, פיתוח או תחזוקה – באחריות מנהל הפרויקט לוודא ערבול של נתונים בפרק זמן סביר (24/48 שעות)

שימוש בנתוני מאגר אישי רגיש שלא בסביבת הייצור (Production) - מותר אך ורק בסביבת טרום יצור (Pre-Production) המנוהלת ברמת אבטחת מידע זהה לייצור.
במקרים בהם מאגר מידע או חלקים ממנו חייבים, מסיבות כלשהן, להישמר במבנה המקורי ללא ערבול, באחריות מנהל הפרויקט לוודא הצפנה ייעודית או הצפנה ביומטרית ולשמור את המאגר במדיה שאינה מחוברת לרשת.

4.1.13 – אחריות לפי סוג השירות

שירות באתר הלקוח
כאשר הלקוח הוא בעל המאגר והמאגר מצוי באתרי הלקוח – הלקוח הוא האחראי לקביעת מדיניות אבטחת המידע למאגר. פעולות הפיתוח, הבדיקות, התחזוקה והתמיכה – המבוצעות ע"י צוות ממוסט, יבוצעו בהתאם להנחיות הלקוח ולמדיניותו.

שירותי גורם חיצוני למאגרים בבעלות מוסט
פיתוח ותחזוקה של מערכות פנימיות בבעלות החברה המבוצעים ע"י קבלן משנה יהיו כפופים לאותן הגבלות החלות על החברה.
במקרים שמוסט נותנת לנותן שירות חיצוני ("גורם חיצוני מורשה") לגשת לנתוני מאגר קיים, חובה על מנהל המאגר לבחון, לפני מתן ההרשאה, את הסיכונים להגנת הפרטיות ואבטחת המידע הכרוכים בהתקשרות עם גורם חיצוני בכלל ועם הגורם החיצוני הספציפי.
בהתאם לסיכונים, עליו לקבוע בהסכם עם הגורם החיצוני (או לוודא קיום הסכם עם הגורם החיצוני) את הנושאים הבאים לפחות:

- מטרות השימוש המותרות לצורכי ההתקשרות
- מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;
- המידע שהגורם החיצוני רשאי לעבד
- סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;
- משך ההתקשרות
- אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע;
- הנחיות לאבטחת מידע
- דרך הדיווח המוסכמת, למילוי חובת התקנות לדווח, לפחות אחת לשנה, לבעל מאגר המידע על אופן ביצוע חובות הגורם החיצוני לפי תקנות הגנת הפרטיות וההסכם ולהודעה לבעל המאגר במקרה של אירוע אבטחה;

באחריות מנהל המאגר לוודא כי הגורם החיצוני החתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם.
באחריות מנהל המאגר לבקר ולפקח אחר מילוי הוראות ההסכם והתקנות ע"י הגורם החיצוני.

במקרה שהגורם החיצוני המורשה מקבל שירות הכרוך בגישה לנתוני המאגר מגורם נוסף, באחריות מנהל המאגר ליידע את הגורם החיצוני כי עליו (על הגורם החיצוני) לקיים הסכם עם הגורם הנוסף בהתאם להנחיות סעיף זה, כאילו הגורם החיצוני הינו בעל המאגר והגורם הנוסף הינו הגורם החיצוני, ולדווח למנהל המאגר על יישום הנחיה זו.
מידע על ההסכם (הפניה) יתועד במסמך הגדרות המאגר

קבלת שירות ב Data Center

במקרים שמוסט הינה גורם חיצוני שנשכר ע"י לקוח לפתח או להטמיע מערכות מידע או לתמוך ולתת שרות למערכות מידע שבבעלות הלקוח, והשרות כולל גם אירוח בחוות השרתים, באחריות "בעל המאגר" (לקוח הקצה) למסור למנהל הפרויקט ממוסט הנחיות לשימוש במאגר (אם המאגר כולל נתוני מידע אישי רגיש)
באחריות מנהל הפרוייקט במוסט להעביר ל Data Center את ההנחיות שקיבלה מוסט מהלקוח בדבר השימוש המותר במאגרי המידע.
לצורך כך יכין "מסמך הנחיות לעבודה עם מאגר" (נספח ב') ויתעד בו את מורשי הגישה למאגר בחברה.
בהיעדר הנחיות מהלקוח ישמשו ההנחיות שבנספח ב' כברירת מחדל ומנהל החטיבה/הפרויקט יקבע את מורשי הגישה על פי מדיניות ניהול המשתמשים בחברה.

4.1.15 שמירת תיעוד ורשומות:

מידע שנאסף בקשר ליישום הוראות תקנות הגנת הפרטיות - ובכלל זה תיעוד אירועי אבטחת מידע, מידע בדבר אבטחת תקשורת, הרשאות גישה, תהליכי זיהוי ואימות ועוד – יישמר למשך שנתיים או לפי הסכם עם לקוח (הארוך מביניהם) .

4.1.16 הדרכה ומודעות:

- חובה על מנהל המאגר לוודא כי מורשי הגישה למאגר יעברו הדרכה לפני קבלת הרשאת גישה. ההדרכה תכלול, לכל הפחות:
- - מעבר על מסמך הגדרות המאגר בדגש על מטרת המאגר ופעולות מותרות/אסורות לביצוע
- - הוראות אבטחת המידע לפי נוהל זה
- - הוראות אבטחת המידע ע"י נספח ב'
- רענון הדרכה יבוצע אחת לשנה ע"י מנהל המאגר ויתועד.
- בעלי גישה למאגר יחתמו על **התחייבות עובד להגנה על מידע פרטי** המופיע בנספח ב' באחריות מנהל המאגר / או מנהל היחידה המחזיקה את המאגר לפי העניין.

4.2 אבטחה פיזית וסביבתית

מאגרי המידע שבבעלות מוסט או המוחזקים על ידה, ינוהלו במרכז המחשבים של מלם (Data Center) הכולל מערכות הגנה וגיבוי לתשתיות ולמידע ונהלי עבודה לתפעול ולתפעול בחירום.
מאגרי מידע המוחזקים ע"י מוסט שאינם בבעלותה ינוהלו באתרי מוסט השונים או באתרי הלקוח או בענן, בהתאם להנחיות הלקוח בהסכם השרות עם מוסט.

4.2.1 בקרות כניסה למתקני החברה:

הכניסה לבניין תהיה באמצעות כרטיס מגנטי מקודד למורשים בלבד.
עמדת השמירה תהיה מאוישת 24 שעות, שבעה ימים בשבוע. באחריות השומר לנעול את דלת הכניסה לבניין בכל מקרה של היעדרות מעמדת השמירה.
עובדים יכנסו לבניין באמצעות כרטיס מגנטי אישי שניתן למורשים בלבד על פי אזורי הרשאה.
אורחים יכנסו למשרדי החברה רק לאחר הזדהות ורישום אצל השומר – ובליווי המארח.
עובדים או קבלנים אשר קיבלו הרשאה לחניה בתחומי הבניין רשאים להיכנס עם רכבם לחניון בו הכניסה מפוקחת באמצעות מצלמות המזהות רכב מורשה או ע"י השומר.
הכניסה מהחניון לבניין תהיה רק באמצעות כרטיס מגנטי אישי.
הליך זה מנוטר ומבוקר באמצעות הטלוויזיה במעגל סגור אשר בעמדת הקבלה.

4.2.2 הכניסה לאזור מרכז המחשבים

הכניסה לאזור מרכז המחשבים בקומה 1 ב Data-Center בירושלים, או לחדרי תקשורת ושרתים במשרדי החברה בפ"ת הינה למורשים בלבד.
אזור ה Data-Center בו מאוחסנים מאגרי המידע הינו אזור סגור לכלל העובדים, למעט עובדי מרכז המחשבים ואחרים על פי הצורך התפקודי.
פתיחת הדלתות הינה באמצעות כרטיס עובד מגנטי ממודר. רק עובדים שאושרו ע"י על ידי מנהל מרכז המחשבים או מנהל מערכות המידע יוכלו להיכנס לאזור מרכז המחשבים.
הכנסת עובדים שאין להם אישור קבוע, אורחים בליווי עובדים וספקים הבאים לבצע עבודות, תהיה ע"י פתיחת הדלת מבפנים ע"י בעלי הרשאה, ורק לאחר שווידואו כי ניתן נוכחותם באזור הינה צורך תפקודי.

4.2.3 הכניסה לחוות השרתים

הכניסה לתוך מתחם Data Center (אולמות השרתים והתקשורת בירושלים) תתאפשר לעובדים בודדים, מורשים בלבד, באמצעות אמצעי בקרת כניסה ביומטרית (טביעת אצבע) ועל בסיס הצורך התפעולי, צרכי התפקיד ורמת סיווג המידע.
באחריות מנהל Data Center לסקור תקופתית את רשימת המורשים ולהורות על גריעה או הוספה של מורשים בהתאם לשינויים.
מנהל התחזוקה של מרכז המחשבים ינהל ויתעד את ההרשאות באמצעות מערכת ניהול הבניין.
רשומות המידע שבמערכת ישמרו למשך שנתיים לפחות.
בכניסה למתחם תופעל מצלמה במעגל סגור שתאפשר לצפות בנכנסים והיוצאים מהמתחם, וכן תאפשר תיחקור בדיעבד במקרה של אירוע אבטחת מידע.

4.2.4 מידע ממצלמות אבטחה

התקנת המצלמות תהיה בהתאם לצורך התפקודי ולסיכונים ובכפיפות למידתיות, סבירות תום לב והגינות, גם כאשר התקנת המצלמות היא תוצאה של דרישת לקוח או נדרשת למילוי חובות רגולציה וחוק.

השימוש במידע המצולם יהיה רק לצורך התפעולי. הקלטות ממצלמה שהותקנה לצורך בקרת כניסה, לא תשמש לצרכי בירור תהליכי משמעת, אלא באישור מנכ"ל ומנהלת משאבי אנוש.

התקנת מצלמות אבטחה טעונה אישור של מנהל תשתית ונכסים במלם.

המידע במערכות הללו יימחק במחזוריות (מידע חדש "יעלה" על מידע ישן)

נספחים

נספח א'	נספח ב'
מסמך הגדרות המאגר	הנחיות לעבודה עם מאגר
מסמך חובה ע"פ תקנות הגנת הפרטיות כאשר מוסט הינה בעל המאגר לאחר המילוי, באחריות מנהל המאגר לתקף את המסמך אחת לשנה ולעדכן בהתאם לממצאי התיקוף	מסמך זה אינו חובה על פי התקנות אך מומלץ להשתמש בו לריכוז הנחיות החברה למחזיקי מאגר ו/או ריכוז ההנחיות להגנת המידע במאגר ספציפי כפי שהתקבלו מבעל המאגר ומחייבות את מחזיק המאגר. כולל גם **טופס התחייבות עובד להגנה על מידע פרטי**
נספח ג'	נספח ד'
כתב מינוי למנהל מאגר	רשימת תיוג לבקרת הגדרות המאגר
טופס מינוי למנהל מאגר – מבוסס על טופס רשמי מחייב של הרשות להגנת הפרטיות.	רשימת תיוג לתיקוף מסמך הגדרות המאגר. חובת התיקוף חלה על מנהל מאגר שבבעלות מוסט, אחת לשנה.
נספח ה'	
טופס תיעוד טכנולוגי מבנה המאגר	
טופס השלמה למסמך הגדרות המאגר, על פי דרישות תקנה 5 – לתיעוד הסביבה הטכנולוגית של המאגר.	