אגף טכנולוגיית מידע ותקשורת

אחריות העובד להגנה על פרטיות ותקנון שימוש מקובל במערכות המידע

גרסה	4.0
נוצר	ספטמבר 2022
עודכן / אומת	דצמבר 2025

1 רקע ומטרות

1.1 המידע המאוחסן במערכות המידע ("נכסי מידע") הוא משאב קריטי ובעל ערך משמעותי לפעילות הג'וינט, לניהול מוצלח של פעילותנו הגלובלית, לשמירה על המוניטין והיכולת שלנו להשיג את משימתנו. כל העובדים וגורמים אחרים המורשים ע"י הארגון, חולקים אחריות להגן על נכסי המידע הללו כדי לשמור על הרמה הנדרשת של סודיות, יושרה, זמינות ושרידות המידע.

1.2 מטרת נוהל זה הינה לקבוע כללי התנהגות ופעולה עבור עובדי הארגון, כדי להגן טוב יותר על נכסי המידע והמערכות של הג'וינט. אבטחת מידע יעילה הינה מאמץ קבוצתי של כל העובדים והשותפים העוסקים במידע ו/או במערכות מידע. באחריותו של כל עובד ואדם מורשה להכיר הנחיות אלו, ולנהל את פעילותו בהתאם.

2 היקף

2.1 ההנחיות בנוהל זה חלות על כל עובדי הארגון וכל אדם מורשה על-ידי הארגון הניגש למערכות המידע או מכשירים טכנולוגיים של הג'וינט.

2.2 הוראות נוהל זה יחולו על –

2.2.1 מכשירים דיגיטליים שסופקו לעובד על ידי הארגון, כולל מחשב נייד, שולחן עבודה, טאבלט, טלפון חכם או מדיה נשלפת.

2.2.2 כל אחת מהיישומים, הפלטפורמות והמערכות של הארגון, כולל דואר אלקטרוני ארגוני.

3 שיטה

3.1 שם משתמש וסיסמה

3.1.1 שמות המשתמש והסיסמאות (ההרשאה) לגישה לרשת ולמערכות של ה-JDC הם אישיים ומיועדים רק לשימושו של העובד, ולביצוע המשימות הקשורות לעבודה.

3.1.2 הסיסמאות חסויות ואסור לשתף או למסור אותן לאף אחד אחר. שיתוף במידע זה אינו נדרש לכל מטרה הקשורה לעבודה.

3.1.3 חל איסור לתעד, להקליט או לשמור סיסמאות במקום שבו הן עלולות להיחשף, למשל, שימוש בפתקים דביקים או בדוא"ל.

3.1.4 במקרה של חשיפת הסיסמה או חשד לחשיפה, יש לשנות את הסיסמה מיד, ולדווח על המקרה לצוות התמיכה של ה- IT (IT Helpdesk).

3.2 התקנה והסרה של תוכנות ויישומים

3.2.1 אסור להתקין תוכנה כלשהי במחשב הארגוני באופן עצמאי. כל התוכנות יותקנו על ידי יחידת ה-IT, לאחר שנבדקו ואושרו מבחינת אבטחת מידע, תאימות ורישוי. יחידת ה-IT תבצע את הרכישה של כל תוכנה נדרשת.

3.2.2 לבקשת התקנת תוכנה במחשב הארגוני, אנא פנו לצוות התמיכה של ה-IT. רק תוכנות הנדרשות לביצוע משימות הקשורות לעבודה יאושרו.

3.2.3 חל איסור להשבית, להסיר או לשנות כל תוכנת אבטחה או קונפיגורציית אבטחה כמו אנטי-וירוס, filewall וכדומה.

3.3 שימוש מאובטח באינטרנט

3.3.1 אסור להעביר, לשמור או לסנכרן מידע ארגוני דרך יישומים מבוססי ענן או אחרים, שאינם של הארגון. כגון: Google Drive, DropBox, Box. אין להשתמש בחשבונות פרטיים לניהול מידע ארגוני.

3.3.2 יש לנקוט באמצעי זהירות סבירים בעת גלישה באינטרנט. הימנע מלחיצה על פרסומות, חלונות קופצים וקישורים לא מאובטחים שעלולים להדביק את המחשב והרשת הארגונית בתוכנות זדוניות (וירוסים, תוכנות זדוניות וכו').

3.3.3 מערכות המידע והנתונים הארגוניים (כולל דואר אלקטרוני, ספריות מסמכים, יישומי Microsoft 365 וכו') הם נכסי הג'וינט, והשימוש בהם מיועד למטרות עבודה בלבד. אין להשתמש בדואר אלקטרוני פרטי ופלטפורמות תקשורת מקוונות אחרות לצרכי עבודה.

3.3.4 השימוש בכתובת האימייל הארגונית לצורך הרשמה לשירותי אינטרנט צריך להיות מוגבל לנושאים הקשורים לעבודה בלבד (למשל, מאגרי מידע מקצועיים, הרשמה לכנסים). אין להשתמש בכתובת האימייל הארגונית שלך כדי להירשם לשירותי אינטרנט למטרות פרטיות.

3.3.5 אין לגשת למידע חסוי או לשנות סיסמה בעת חיבור לרשת Wi-Fi ציבורית, כמו בתי מלון, שדות תעופה, בתי קפה וכו'. ניתן להשתמש בנקודת גישה למכשיר סלולרי במידת הצורך.

3.3.6 חל איסור להשתמש במכשירי הארגון או בתוכנות ויישומים של הארגון לצורך צריכת תוכן בלתי הולם או בלתי חוקי, או תוכן שהושג באופן בלתי חוקי. זה כולל הורדה, התקנה או צפייה בתוכן כזה וביישומים נלווים.

3.3.7 אסור לגלוש ברשת Darknet, כולל שימוש בתוכנות אנונימיזציה.

3.4 שימוש מאובטח בדוא"ל ופלטפורמות תקשורת של הארגון

3.4.1 אין לפתוח הודעות דוא"ל ממקור לא ידוע או חשוד.

3.4.2 אין לפתוח קבצים מצורפים או ללחוץ על קישורים ממקור לא ידוע או חשוד.

3.4.3 אין לפתוח קבצים מצורפים או ללחוץ על קישורים שאינך מצפה לקבל, גם אם המקור נראה לגיטימי.

3.4.4 אם התקבלה הודעת דוא"ל ממקור חשוד או אם אינך בטוח/ה לגבי אמיתות הודעת האימייל, יש דווח על כך מיד לשירות התמיכה של ה-IT.

3.4.5 בעת שליחת הודעת דוא"ל קבוצתית הכוללת גם נמענים חיצוניים, יש להשתמש ב- BCC על מנת להסתיר את כתובות האימייל של הנמענים. שימוש כזה יגביל את החשיפה של כתובות אימייל לספאם ודיוג.

3.4.6 אין לשתף או לאחסן מידע מזהה אישי (PII: Personally Identifiable Information) בפלטפורמות האימייל והתקשורת

הארגוניות.

3.4.7 אם את/ה מקבל מידע אישי מזהה (PII) דרך דואר אלקטרוני, יש לאחסן את הנתונים במקום מאובטח במערכות הארגון (SharePoint ו-OneDrive) ולמחוק אותם מחשבון האימייל.

3.5 שימוש מאובטח בציוד

3.5.1 חל איסור להשתמש במכשירי הארגון או במערכות המידע של הארגון למטרות בלתי חוקיות.

3.5.2 יש להשתמש במכשירי ומערכות המידע של הארגון לצרכי העבודה בלבד.

3.5.3 חל איסור לחבר לרשת הארגון ציוד שאינו של הג'וינט.

3.6 אבטחת ציוד הארגון ונכסי מידע

3.6.1 מכשיר המשמש לגישה למערכות ולנתוני הארגון חייב להיות נעול (מוגן באמצעות סיסמה) כאשר המכשיר נשאר ללא השגחה.

3.6.2 יש להקפיד על הגנה פיזית על המכשירים ולהפעיל שיקול דעת סביר כאשר משאירים מכשיר ללא השגחה. לדוגמה: לא להשאיר מכשיר ללא השגחה במקומות ציבוריים, עם אדם לא אמין, או ברכב.

3.7 מדיה נשלפת ומכשירים חכמים

3.7.1 אסור לחבר התקן אחסון נשלף למחשבי הארגון. מכשירי אחסון נשלפים כוללים כרטיס פלאש, כונן און קיים, דיסק און קי, ומכשיר אחסון קבצים USB.

3.7.2 אין לחבר טלפון חכם למחשבי הארגון כדי לטעון אותו או להעביר נתונים.

3.7.3 אסור לחבר טלפון נייד או מכשירים חכמים אחרים לתחנות עגינה של הארגון.

3.8 הגנה על נכסי המידע של הארגון

3.8.1 נכסי המידע ומוצרי העבודה של הג'וינט שייכים לארגון והם חיוניים להמשך תפעול שירותי ותוכניות הג'וינט. הנתונים צריכים להישמר רק במערכות המאושרות והמאובטחות של הארגון המיועד.

3.8.2 יש להעלות או לסנכרן נתונים רק לשירותי ענן מאושרים ומאובטחים כמו Office 365 של JDC (SharePoint, OneDrive).

3.8.3 ספריות המסמכים של JDC SharePoint ו-OneDrive צריכות להיות מסונכרנות רק במחשבים ארגוניים, ולעולם לא במחשבים אישיים. הגרסאות מבוססות הרשת של SharePoint, OneDrive ו-Teams יכולות לשמש במחשבים אישיים במקום האפליקציה המותקנת.

3.8.4 בעת יצירת דוחות או כל צורה אחרת של ייצוא נתונים מיישומים ארגוניים, קבצי הפלט (e.g. PDF, Excel) חייבים להישמר רק בפלטפורמות המאושרות והמאובטחות של הארגון.

3.8.5 אסור לאחסן מידע של הארגון במדיה נשלפת, כונני דיסק מקומיים במחשבים ניידים או שולחניים, ו/או חשבונות שירותי ענן אישיים, כגון DropBox, Box ו-Google Drive.

3.9 אפליקציות בינה מלאכותית (AI)

בעת השימוש באפליקציות AI, יש לשים לב לסיכונים הבאים:

3.9.1 כל מידע שהועבר או הועלה לאפליקציות בינה מלאכותית יכול להופיע באינטרנט ולהיות נגיש לציבור, בדומה לשיתוף פוסט ברשתות החברתיות. לכן, יש להתייחס למידע כזה כאל הפצה ציבורית.

3.9.2 מידע ששותף עם אפליקציות בינה מלאכותית עלול להשפיע לרעה גם על שותפי הג'וינט ולקוחותיו, להציג את הארגון כאחראי לפגיעה ולגרום נזק למוניטין של הארגון.

3.9.3 מבין אפליקציות הבינה המלאכותית הלגיטימיות הקיימות כיום, יש הרבה אפליקציות AI מזויפות שנועדו לגרום לנו להוריד אותן. אפליקציות AI אלו עשויות להיות משולבות עם תוכנות זדוניות שמטרתן לגנוב את הנתונים שלנו או להתקין תוכנות זדוניות אחרות.

מדיניות שימוש מקובל באפליקציות בינה מלאכותית:

א. יש להבין שאנו, כמשתמשים, אחראים על תוצרי העבודה שנוצרו ע"י בינה מלאכותית באותה מידה שבה אנו אחראים על תוצרי עבודה שנוצרו ללא שימוש באפליקציית בינה מלאכותית.

3.9.4 לפני השימוש באפליקציית AI, יש לדבר עם המנהל/ת שלך על הצורך בשימוש באפליקצייה, ולקבל ממנו/ה אישור להשתמש בכלי.

3.9.5 למעט כפי שנקבע במסמך זה בנוגע לרישיונות הארגון לשימוש ב-Microsoft CoPilot, וכפי שמפורט בסעיף 3.9.20, אין לספק מידע אישי מזהה (PII) לאפליקציות בינה מלאכותית (כולל PII של שותפים, תורמים, משתתפי תוכניות, לקוחות, עובדים או כל אדם אחר).

א. מידע אישי מזהה כולל את שם האדם, גיל, כתובת, דת, מידע בריאותי, מידע פיננסי, מקום לידה, נתוני תעסוקה או תמונה (אם התמונה כוללת חלק או כל פניו).

3.9.6 למעט כפי שנקבע במסמך זה בנוגע לרישיונות הארגון לשימוש ב-Microsoft CoPilot וב-ChatGPT, וכפי שמפורט בפסקה 3.9.20, אין להשתמש בשם הארגון באפליקציית AI (השתמש במונח כללי כמו "ארגון ללא מטרות רווח" או "הארגון שלי") ואין לספק מידע אחר שיזהה את הארגון כארגון הג'וינט.

3.9.7 למעט מה שנקבע במסמך זה בנוגע לרישיונות של הארגון לשימוש ב-Microsoft CoPilot וב-ChatGPT, וכפי שמפורט בסעיף 3.9.20, אין להעלות מידע ארגוני רגיש או סודי, כולל:

א. תוכניות אסטרטגיות (כגון פרטי שותפויות ושיתופי פעולה, אסטרטגיות גיוס כספים וקמפיינים).

ב. מידע פיננסי (כגון מענקים ומקורות מימון, תוכניות תקציב ותחזיות).

ג. תקשורת פנימית ופרוטוקולים של פגישות (כגון מיילים

ותמלולי Teams).

ד. מידע על הלקוחות או התוכניות שלנו.

ה. מידע על עבודתנו באזורים או תוכניות רגישות, כולל עבודתנו ברוסיה, אוקראינה, קובה וסארוואס.

ו. מידע דמוגרפי על הקהילות שאנו תומכים בהן.

ז. מידע על נסיעות קבוצתיות קרובות, כולל תאריכים ומיקומים.

ח. מידע על נהלי האבטחה והפרוטוקולים שלנו.

ט. מידע שעלול לסכן את הבטיחות והביטחון של קהילת הג'וינט.

3.9.8 אין להעלות מדיה עם אנשים או פנים הנתנים לזיהוי.

3.9.9 יש להימנע משימוש במדיה שזכויות הקניין הרוחני שלה אינן בבעלות הארגון. לרב, הארגון יהיה הבעלים של זכויות הקניין הרוחני על תוצרים שנוצרו ע"י עובדי הארגון. יתכן גם שלג'וינט יש בעלות על הקניין הרוחני של יצירות שנוצרו על ידי אחרים. אנא בדקו עם מחלקת Marcom כדי לאמת את זכויות הקניין הרוחני של כל מדיה לפני הכנסתה לכלי AI.

3.9.10 יש להימנע משימוש במדיה שלג'וינט אין זכויות פרטיות מידע כדי לעבד נתונים אלו באמצעות AI, כולל תמונות וסרטונים המכילים אנשים או פנים הניתנים לזיהוי. לארגון בדרך כלל יש זכויות פרטיות מידע להשתמש במדיה עם אנשים או פנים הניתנים לזיהוי רק כאשר הוא מקבל הסכמה כתובה על כך. אם יש לכם שאלות בנוגע לזכויות פרטיות נתונים ובינה מלאכותית, אנא בדקו עם המחלקה המשפטית לפני השימוש.

3.9.11 שימו לב שתוכן שנוצר על ידי AI עשוי להכיל קניין רוחני בבעלות אחרים. לכן, הארגון אינו רשאי להשתמש במדיה כזו ללא רשות. שימוש בתוכן שנוצר על ידי בינה מלאכותית ללא אישור בעלי קניין רוחני עלול לחשוף את הג'וינט לתביעות משפטיות בגין גניבת קניין רוחני. אם יש לך שאלות לגבי קניין רוחני ותוכן שנוצר על ידי בינה מלאכותית, אנא בדוק עם המחלקה המשפטית לפני השימוש.

3.9.12 יש לאמת תוכן שנוצר על ידי בינה מלאכותית, במיוחד עובדות, ולבדוק את מהימנות המידע על ידי הצלבה עם מקורות שאינם מבוססי בינה מלאכותית כמו מנוע חיפוש מבוסס אינטרנט או מסד נתונים ציבורי אחר ממקור אמין.

3.9.13 בינה מלאכותית אינה תחליף למומחיות פנימית וחיצונית. אסור להשתמש בבינה מלאכותית כתחליף לייעוץ עם מחלקות רלוונטיות בארגון, כולל מחלקות המשפטים, הכספים ומשאבי אנוש.

3.9.14 בינה מלאכותית אינה מקור אמין בכל הנוגע להיסטוריית ארגון הג'וינט. כל המידע ההיסטורי הארגון צריך להיות מאומת עם מחלקת הארכיון.

3.9.15 שימוש בכל אפליקציית בינה מלאכותית דורש אישור IT לפני השימוש. בכל בקשה, יש לפנות לתמיכה הטכנית של צוות ה-IT.

3.9.16 אם יש לך חשדות לגבי הלגיטימיות של אפליקציית AI, יש לפנות לתמיכת ה-IT עם שאלתך. הינך האחראי/ית על השימוש בכלי AI בכל הקשור לארגון או מערכות הארגון.

3.9.17 אין להשתמש בכלי בינה מלאכותית כדי להעריך מועמדים לעבודה,

כולל לניוד פנימי או קידום, או לקבלת החלטות תעסוקתיות אחרות.

3.9.18 בעת שיתוף פעולה עם ספקים וקבלנים, יש מראש לבדוק עם הספק האם כלי בינה מיושמים בשירות שהם מספקים. הספק או הקבלן חייבים להסכים להוראות מדיניות השימוש המקובל הנוגעות לעיבוד מידע רגיש של הארגון ולכל מידע אישי שמספק הארגון. במידת הצורך, המחלקה המשפטית תוסיף נוסח רלוונטי לחוזה עם הספק. אם אתם מתכוונים שספקים ישתמשו בכלי בינה מלאכותית בשם הארגון, אנא פנו למחלקה המשפטית.

3.9.19 בעת שימוש ב-AI, על עובדי הג'וינט להקפיד על הנחיות והנהלים האחרים בהתאם למדיניות הג'וינט, לרבות מדיניות הג'וינט הקשורה להקלטת פגישות.

3.9.20 שימוש בכלי AI מאושר ומורשה על ידי הג'וינט:

א. **Microsoft CoPilot**: CoPilot של דפדפן Microsoft Edge על מחשב נייד ארגוני עם משתמש ארגוני: אפליקציה זו מספקת אבטחה נוספת לנתוני הארגון, כך שתוכל/י להשתמש במידע ארגוני ומידע אישי מזהה (PII).

ב. **ChatGPT ברישיון JDC**: אפליקציה זו מספקת אמצעי אבטחה מוגבלים, ולכן מותר להעלות מידע ארגוני (למשל, שמות תוכניות ותקציבים); עם זאת, אין להעלות מידע אישי מזהה (PII) בשום פנים ואופן.

4 חובת דיווח

4.1.1 כל אירוע אבטחת מידע או אירוע חשוד באבטחת מידע חייב להיות מדווח מיד ל-IT Helpdesk.

4.1.2 להלן דוגמאות לאירועי אבטחת מידע פוטנציאליים:

- גניבה או אובדן של מכשיר ששימש לניהול או גישה לנתוני הארגון, לדוגמה, מחשב נייד או מכשיר חכם – גם אם אינו מכשיר הארגון.
- כל ניסיון חשוד להוציא מידע מעובד.
- שינויים חריגים או בלתי מוסברים בהתנהגות המכשיר והתוכנה (תנועות עכבר בלתי צפויות, הופעת תוכניות או קבצים לא ידועים, התנהגות או חוקים בלתי צפויים באפליקציית הדואר של Outlook, התראות אנטי-וירוס וכו').
- קבלת דוא"ל חשוד או הודעות אחרות שמטרתן לחלץ מידע חסוי או פרטי משתמש (פישינג).
- חשש או חשד שהמידע המאוחסן במערכות נפגע (נמחק, שונה או נחשף).
- כל כשל אבטחה פיזי שעלול לסכן חומרה או נתונים (יש להודיע גם לקציין האבטחה של JDC וגם ל-IT Helpdesk).

5 ביצוע

5.1 ארגון הג'וינט יבצע ניתור ובקרה של הרשת, תוכנות ומכשירי של הארגון כדי למנוע אירועי אבטחת מידע, בהתאם לחקיקה ולתקנות המקומיות.

5.2 לצורך אבטחת מידע על מכשירים ועל הרשת הארגונית, הארגון עשוי למחוק את כל או חלק מהמידע המאוחסן במכשיר במקרה של אובדן, גניבה, ניצול לרעה או חשד לפגיעה.

5.3 כל עובדי הג'וינט ואנשים מורשים אחרים מחויבים לעיין ולחתום על מדיניות זו.

5.4 הפרת הוראות הליך זה עלולה להוות עבירה משמעתית ועלולה להוביל לפעולה משמעתית נגד העובד.