

פרויקט IDM

מפת"חון זה נועד לסייע לארגון בהתנעת הפרויקט ומהווה מסגרת כללית לאפיון הדרישות וביצוע המיפויים הנדרשים כחלק מההערכות הארגוניות לביצוע הפרויקט.

פרויקט IDM הינו פרויקט מורכב עם רמת אינטגרציה ותיאום גבוהים, הן טכנולוגית, בין מערכת IDM ל-AD, ולמערכות שאינן סטנדרטיות, והן מבחינת תהליכי עבודה ואתחול המערכת עם משאבי אנוש, אבטחת מידע ויחידות עסקיות.

מתודה ממליצה על 10 השלבים הבאים לביצוע מוצלח של הפרויקט:



1. הגדר את יעדי הפרויקט - ניהול הרשאות מרכזי? ייעול תהליכים ארגוניים? שיפור רמת אבטחת מידע?
2. חשיבות הגורם האנושי - 80% מהצלחת הפרויקט מושפעים משיקולים ארגוניים. רק 20% מושפעים מטכנולוגיה. תמיכת הנהלה הכרחית!
3. הגדר את גבולות הפרויקט - אילו מערכות נכללות בתכולת הפרויקט ולא פחות חשוב מה לא נכלל?
4. מפה תהליכים עסקיים וטכנולוגיים.
5. Data Cleaning - משתמשים והרשאות לא פעילים, משתמשים ללא הרשאות, הרשאות ללא משתמשים.
6. Role Mining - שאיפה להגיע למספר פרופילים מצומצם, כדי להשיג ניהול יעיל ופשוט של הרשאות.
7. נתח תהליכים נדרשים - מי מאשר? מה? מתי? למה? מי מבצע? בד"כ זו תורה שבעל פה בארגון.
8. הגדר ארכיטקטורה נדרשת.
9. בחר ספק / טכנולוגיה.
10. התחל בפרויקט.

נשמח לשתף אתכם ב- Best Practices שהצטברו במתודה בניהול פרויקטי IDM מקצה לקצה, משלב ניתוח צרכים, דרך סיוע במיפוי וטיוב נתונים, ניהול מרכז מסודר לבחירת ספק מתאים, ולבסוף ליווי הפרויקט בתהליך המימוש וסיוע בהטמעה.

- <סיווג המסמך> -

זכויות היוצרים של מוצר זה או תבנית זו הן של חברת מתודה מחשבים בע"מ המוצר/התבנית ניתנים לשימוש אישי שימוש מסחרי מחייב רישוי מפת"ח עמ' 1 מתוך 5

מפת"חון להקמת מערכת IDM

שם האפליקציה:	תאריך עדכון המסמך:
מנהל הפרויקט:	

1. יעדים

לקוח

מי מבקש את הפרויקט, (מממן, מתקצב?), מי עתיד לתפעל את המערכת בשוטף?.

יעדים ומטרות הפרויקט

יש להגדיר בצורה ברורה את היעדים והמטרות של הפרויקט. ראה דוגמא ליעדים ומטרות עיקריים לפרויקט IDM במדריך של קיט ניהול זהויות

סיכונים

יש לפרט את הסיכונים העסקיים והתפעוליים שעלולים לפגוע בפרויקט. ראה דוגמא לסיכונים עיקריים לפרויקט IDM במדריך של קיט ניהול זהויות

עלות תועלת

מהם התועלות והסיכויים העסקיים? (יש לנסות לכמת עד כמה שניתן את יחס העלות/תועלת)

2. יישום

מילון מונחים

מערכות IDM שונות משתמשות בטרמינולוגיה שונה לחלק מהמושגים. רצוי לצרף מילון מונחים מקובלים בשימוש בתחום IDM. ראה דוגמא למונחים עיקריים במערכות IDM במדריך של קיט ניהול זהויות

מצב קיים

תיאור אופן תפעול והגדרת ההרשאות במצב הקיים.

מיפוי של סוגי משתמשים ברמת התפקידים השונים בכל יחידה אירגונית. המיפוי ישמש כבסיס לבניית ROLE במערכת ה-IDM. למיפוי יש להוסיף "משתמשים" שאינם משתייכים לעובדים (למשל, משתמשים שנוצרו עבור הרצת ג'ובים או שירותים בייצור, משתמשים שנועדו לגישה לבסיס נתונים ע"י אפליקציה וכדומה).

התייחסות להפרדת סמכויות בביצוע פעילויות שונות. כתוצאה מכך, יתכן שיידרש להגדיר לעובדים באותה יחידה אירגונית תפקידים שונים.

#	יחידה אירגונית	תפקיד	מספר משתמשים	תיאור/הערות
1				
2				

- <סיווג המסמך> -

מיפוי המערכות העיקריות בארגון הכוללות הזדהות בכניסה כולל החלטה אם נכללות בסקופ הפרויקט או לא.

יש לבדל בין מערכות אשר מבצעות הזדהות מול AD, לבין מערכות אשר מנהלות פנימית משתמש/סיסמא (עבורן נדרשת החלטה אם לעבור להזדהות מול AD או להגדיר את הממשקים המתאימים מול מערכת ה-IDM).

שם מערכת	תיאור קצר	ניהול בסיס נתוני משתמשים פנימי?	הזדהות מול AD?	בסקופ הפרויקט?

תהליכים בהם המערכת נדרשת לתמוך

מיפוי כלל התהליכים שיש להם השפעה על הרשאות העובד, בהם המערכת נדרשת לתמוך (לדוגמא: קליטת עובד חדש, שינוי תפקיד, כניסה לחל"ד - חופשת לידה, חל"ת - חופשה ללא תשלום, שינוי הרשאות לעובד קיים, סיום עבודה וכו').

מיפוי פעילויות נדרשות להשלמת סביבת העבודה של העובד בין אם מתבצעות באופן אוטומטי או ידנית לפי בקשה (לדוגמא: הגדרת Home Dir, הגדרת מייל אירגוני, פתיחת הרשאות לבסיסי נתונים, פתיחת הרשאות ל-LINUX/UNIX, פתיחת הרשאות לפרטל אירגוני וכדומה).

מיפוי רגולציות שהארגון נדרש לאכוף כולל התייחסות לאופן הטמעת אכיפתן.

מיפוי סבב אישורים נדרש עבור כלל התהליכים הרלוונטיים.

ממשקים

מיפוי ממשקים נדרשים בין מערכת ה-IDM למערכות חיצוניות.

אם אפשר לפרט בשלב זה, מומלץ לציין את אופן ההתממשקות כגון WS, ממשק XML וכו'.

מיפוי הרשאות ברמת תפקיד לכל יחידה

מיפוי מערכות שבשימוש כל תפקיד בכל יחידה.

שם מערכת	מנהל סוג 1	מנהל סוג 2	מזכירה	עובד סוג 1	עובד סוג 2	עובד סוג 3

אילוצים

תיאור אילוצי מערכת, אילוצים עסקיים ואחרים.

דו"חות

מיפוי הדו"חות הנדרשים מהמערכת. להלן דוגמאות לדו"חות עיקריים:

- <סיווג המסמך> -

זכויות היוצרים של מוצר זה או תבנית זו הן של חברת מתודה מחשבים בע"מ המוצר/התבנית ניתנים לשימוש אישי שימוש מסחרי מחייב רישוי מפת"ח עמ' 3 מתוך 5

- א. דו"ח המפרט פעילות כללית לתקופה מוגדרת, כולל חשבונות שיוצרו, חשבונות שנמחקו, פעולות יזומות שנעשו במערכת וכדומה.
- ב. דוחות סטטוס כגון : דוח חשבונות משתמשים בחתך מערכות מנוהלות ויחידות ארגוניות, דוח מערכות והרשאות המקושרות לזהות ספציפית, דוח משתמשים להם גישה למערכת ספציפית.
- ג. דוחות חריגים כגון : חשבונות משתמשים במערכות המקושרות אשר אינם מקושרים לישות במערכת ניהול הזהויות, דו"ח המפרט חשבונות משתמשים לא פעילים X חודשים.

אבטחת מידע

☞ התייחסות לדרישות אבטחת מידע בנושאים העיקריים הבאים :

- א. זיהוי - אמצעי הזיהוי של עובד, התייחסות לזיהוי חכם למשל עבור הוצאת הדפסות וכו'.
- ב. גישה מרחוק לשירותי המערכת - על בסיס נוהל גישה מרחוק של עובד הארגון/ספק חיצוני.
- ג. מידור הרשאות - הוראות אבטחת מידע הנוגעות להגבלת הרשאות עובדים.
- ד. הרשאות ביצוע - הוראות אבטחת מידע בנוגע להרשאות חריגות לביצוע פעילויות במערכות השונות.
- ה. התראות - דרישות להתראות אוטומטיות של המערכת על חריגים.
- ו. תיעוד ולוג - הגדרת דרישות בנושאים העיקריים הבאים :
 - מנגנון מעקב (Auditing) פנימי, אשר יתעד את פעילות משתמשי המערכת.
 - אפשרות קישור למערכת השו"ב הקיימת.
 - אפשרות לביקורת log נוחה וידידותית מממשק המערכת או בכל דרך אחרת ידידותית לתפעול.

3. טכנולוגיה ותשתית

☞ תיאור הארכיטקטורה הלוגית הנדרשת והגדרת דרישות החומרה, התוכנה, שו"ב, גיבוי, שרידות והתאוששות, זמינות וכו'.

4. מימוש

גורמים מעורבים

☞ הגורמים המעורבים מטעם הארגון ומטעם הספק ברמת ביצוע והיגוי (כולל גורמים חיצוניים אם יש).

תכנית עבודה

☞ אבני הדרך העיקריות בפרויקט ה-IDM כולל חלוקה לשלבים במידת הצורך על פי עדיפויות.

☞ כיצד מתוכנן לבצע את הבדיקות - סביבת בדיקות כולל ממשקים למערכות, מי מבצע את הבדיקות? האם מתוכנן פיילוט?

- < סיווג המסמך > -

הדרכה והטמעה

- ☞ כיצד תבוצע ההדרכה למשתמשים שאמורים לתחזק את המערכת בשוטף?
- ☞ התייחסות להטמעת שינויים בתהליכי העבודה בארגון עקב הכנסת המערכת.

שירות ותחזוקה

- ☞ הגדרת דרישות לתקופת האחריות (בד"כ שנה) ולתקופת התחזוקה - איזה שירות מצפים מהספק, באיזה SLA וכו'.

5. עלות

עלות הקמה (משוערת)

- ☞ מהן העלויות הקשורות בהקמת המערכת כולל עלויות רכש שרתים, רישיונות, עלויות הגורמים המעורבים לפי שלבי מחזור חיים, שעות ניהול, וכו'.

עלות שוטפת - תחזוקה (משוערת)

- ☞ מהן העלויות הנדרשות לתחזוקת המערכת.

- < סיווג המסמך > -

זכויות היוצרים של מוצר זה או תבנית זו הן של חברת מתודה מחשבים בע"מ
המוצר/התבנית ניתנים לשימוש אישי
שימוש מסחרי מחייב רישוי מפת"ח
עמ' 5 מתוך 5