מאת: דרור ארפי <DrorA@court.gov.il>
אל,<nisimtza@mof.gov.il> "nisimtza@mof.gov.il" :
תאריך: 13:02 26/05/2014
נושא :FW מסמך דרישות הנהלת בתי המשפט

לבקשתך, להלן התייחסות

בברכה,
דרור ארפי | מנהל תפעול ושירות | אגף מערכות מידע ומחשוב | הנהלת בתי המשפט
משרד: 02-6556784 | נייד: 050-6256784 | פקס: 02-6556753 |Drora@court.gov.il

-----Original Message-----
From: אהוד בן משה
Sent: Monday, May 26, 2014 12:58 PM
To: דרור ארפי
Cc: דייויד קסטיאל; ירדן ירדני
Subject: RE: מסמך דרישות הנהלת בתי המשפט

להלן רשימת הדרישות המופיעות במסמך והתייחסות לנושא mdm באופן כללי כל דרישות הסף נתמכות ע"י A.W

כללי אכיפת מדיניות ובקרה - תומך

1. תאימות מלאה לכלל היצרנים והמכשירים הקיימים - 2. ניהול של כל מערכות ההפעלה המובילות: iOS, Android, Windows Mobile 7, BlackBerry, Symbian - 3. תמיכה בעברית - 4. זיהוי מערכת הפעלה, גרסת התוכנה ואפליקציות מתקנות - 5. זיהוי מכשירים שעברו Jail Break או Rooted ולהתריע על כך כחלק מבדיקת המדיניות - 6. מניעת סנכרון כתוצאה מאי עמידה במדיניות המכשיר בודק את ההגדרות שניתנו במידה וישנו ניסיון לשנות את ההגדרות, האירוע ידווח ותיתכן מניעת גישתו לרשת החברה ואף מחיקה מרחוק - 7. בקרה על סוגי המכשירים המותרים לסנכרון - 8. אכיפת מדיניות כללית - מניעת הסרת ה Client ע"י המשתמש, הסרה של סוכן רק ע"י סיסמת מנהל - 9. אכיפת מדיניות אפליקציה שליטה על אפליקציות הנמצאות במכשיר החכם - 10. הגבלה על הורדת אפליקציות ע"י שימוש ב- whitelists and blacklists - 11. בקרה על גישה לחנות האפליקציות ואיסור על הורדת אפליקציות באופן ישיר ללא אישור - 12. בקרה על גישה לשימושי WEB , רשתות חברתיות , הורדת אפליקציה של בהתאם למדיניות - 13. בקרה וחסימת סוגי קבצים המגיעים בצרופות - 14. בקרה והגבלת הודעות דוא"ל ע"פ נפחים - 15. אכיפה מדיניות תקשורת סלולארית חיסכון בעליות מתן יכולות לדווח על שימוש חריג במכשיר - 16. בקרה על שימוש ב- Roaming מעבר בין רשתות סלולארית בחול - 17. זיהוי הפרת המדיניות ונקיטת פועלה או ושלחת התראה ל IT - ולמשתמש עדכון מצב חשבון בזמן אמת - 18. אכיפה מידניות הפרדה בין מידע אישי למידע ארגוני מערכת האבטחה תאפשר באמצעות מתן יכולת ניהול המידע על פני סוגים שונים של הסכמי חלוקה של מכשרים עובד יוכל להביא מכשיר מהבית ובו להכניס מידע ארגוני או עובד השומר מידע פרטי ע"ג מכשיר ארגוני. המערכת תתמוך בשתי התצורות בהתאם לחוזי העסקה של העובדים - 19. ניהול אפליקציות ארגוניות במכשיר פרטי או אפליקציות פרטיות במכשיר ארגוני - 20. סימון מידע אירגוני או פרטי - 21. כאשר ישנו שימוש בחבילה סגורה Sandbox תוכנה נפרדת למערכת סנכרון הדואר ואפליקציות הארגונית יש לוודא כי לא ניתן לעביר מידע ממכשיר הטלפון החכם לSandox ולהפך-

אבטחת מידע - תומך

1. הזדהות למכשיר תתבצע באמצעות סיסמא או אמצעי אחר כגון תביעת אצבע תלוי ביכולת
הטכנולוגית במכשיר החכם אשר נדרש לתמוך במדיניות הסיסמאות בארגון למכשיר טלפו חכם - 2. יכולת נעילת המכשיר לאחר פרק זמן שלא נעשה שימוש במכשיר. הגישה

למכשיר תחייב
הזדהות מחדש-
3.יכולת שימוש ב Certificate ייעודי לטובת זיהוי המכשיר מול רשת החברה - 4. יכולות של Backup, Wipe, Selective Wipe המערכת תדע לבצע מחיקה מלאה, מחיקה חלקית וגיבוי של המידע הקיים במכשיר - 5. יכולת הצפנת המידע העסקי הרגיש הקיים במכשיר החכם ובכרטיס הזיכרון על מנת למנוע גישה לא מורשית במקרה של אובדן או גניבה - 6. מחיקת תוכן המכשיר אוטומטית אחרי מס' ניסיונות גישה כושלים למכשיר - 7. זיהוי אפליקציות זדוניות - 8. אנטי וירוס מבוסס עדכון חתומות ע"י יצרן מוכר - 9. ארכוב הודעות SMS , IM , email וכו'(לשם שימוש בדוחות ו. Audit trail -
10.הצפנת המידע הפנימי והצפנת המידע בתנועה - 11. מחיקה סלקטיבית מרחוק-
12.מידע ארגוני לא יעבור בין חבילת ה Sandbox לבין המכשיר החכם - 13. בממשק הדואר בקרה על צירוף קבצים Attachments למכשיר לדוגמא: חסימה של שליחת Attachmentsמהארגון או מתן אפשרות רק לסוגי קבצים כמו PDF,JPEG 14. חסימה משלוח הודעות דוא"ל פנימיות מתן אפשרות לקבל למכשיר רק הודעות דוא"ל שנשלחו מחוץ לארגון, ומניעת קבלת הודעות דוא"ל מתוך הארגון

<u>ניהול מרכזי - תומך</u>
1.ממשק שליטה וניהול המידע המוצג במערכת יהיה מקיף ויכלול את כל הנתונים לגבי כל הטלפונים החכמים בארגון.
2.הפצת Policy ארגוני המערכת תדע להפיץ מדיניות ארגונית אחידה או פרטנית בהתאם לסוג המכשיר או המשתמש.
3.ניהול מלאי המכשירים הקיים בארגון המערכת תדע לזהות את כלל המכשירים הקיימים בארגון, ברמת חומרה ותוכנה.
4.ניהול גרסאות מעת לעת משיקות יצרניות הטלפונים גרסאות חדשות למערכות ההפעלה, הגרסאות החדשות מתקנות ליקויים טכניים ואבטחתיים שנתגלו בגרסאות הקיימות
למכשירים ומערכות ההפעלה בהתאם לצורכי הארגון - 5. הפצת Client המערכת תדע לתמוך בהפצת Client - באמצעות SMS או Email או בעזרת שימוש ב APP STORE של Appleו Android Market של 6. - Google יכולת חסימה של התקנים או ממשקים(, Infrared , Bluetooth , Wi-Fiמצלמה - 7. השמדה מרחוק יכולת למחוק את המכשיר במקרה של דיווח על אובדן או גניבה - 8. המערכת תוודא אחת לפרק זמן שיקבע את הגדרות האבטחה ואימות במכשיר - 9. המערכת תתמוך במדיניות גרנולארית במקרה של חוסר עמידה במדיניות הארגון - 10. יכולת איתור מכשיר טלפון חכם אבוד ע"י הצגת מיקום ע"ג מפה, ושחזור הגדרות בעת מציאתו-

Help Desk תומך
1.ממשק ניהול יחיד מבוסס- WEB
2.מספר רמות הרשאה לניהול-
3.יצירת דוחות-
4.מתן התראות על אירועים חריגים-
5.שליטה מרחוק יכולת לשלוט על המכשיר מרחוק, במקרה של תקלה ותאפשר מתן תמיכה בהגדרות וגיבוי מידע - 6. תפעול ברמת משתמש והתקנה והסרה של תוכנה ע"י המכשיר החכם בהתאם לממקש היצרן - 7. תמיכה בשירות עצמי - 8. תמיכה ביכולת ניתור מקצה לקצה - 9. כלי טיפול בתקלות - 10. התראות - התממשקות למערכות המידע הארגוניות - 5.1 Blackberry 4. LDAP 3. Exchange 2. Active Directory . Monitoring 6. Siem

- SIM תומך
1.יכולת מחיקת המכשיר במקרה של החלפת הSIM -
2.במקרה של החלפת , SIM סביבת העבודה במכשיר נשארת מוגנת ולא ניתן לגשת לחומרים שהוגדרו רגישים

בברכה,
אגף מערכות מידע ומחשוב | הנהלת בתי המשפט| מנהל טכנולוגי | אהוד בן משה
026556753: | bme@court.gov.il פקס| 052-3628705נייד: | 02-6556875
משרד: