

חיצוניים ספקים על פיקוח חובת

אבטחה פיזית (אמצעי פיקוח טכניים)

מדוע זה חשוב	תיאור הפיקוח	כותרת פיקוח
<p>שמירה על מערכת בקרת גישה יעילה, כמו גם על תהליכים והנהלים הנדרשים לניהול גישה הם מרכיבים חיוניים במסגרת מערכת פיקוח רב-שכבתית הנדרשת כדי להגן על האזור מפני גישה בלתי מורשית ועל מנת לוודא שהנכסים מאובטחים ומוגנים. אי קיום אמצעים יעילים לניהול בקרת גישה עלול להוות סיכון שיובייל לכניסה של עובדים בלתי מורשים לאתרי הספק או לאזורים מוגבלים בתוך אתרי הספק. הדבר עלול להגביר את הסיכון לאובדן או לפגיעה בנכסים של Barclays ואף לגרום להפסד כספי ונזק למוניטין ו/או השתתה של קנס/סנקציה מצד הגורם הרגולטורי.</p>	<p>יש להגדיר כללי בקרת גישה עבור כל האזורים המאובטחים, תוך יישום תמיכה של נהלים רשמיים מאושרים ותחומי אחריות מוגדרים.</p> <p>יש להגן על אזורים מאובטחים באמצעות התקנת בקורות כניסה ונקודות גישה מתאימות. תוך שימוש בפתרונות בקרת גישה אלקטרוניים, מכניים או דיגיטליים.</p> <p>יש להגביל גישה לוגית ומנהלית למערכות בקרת גישה אלקטרוני לאנשי צוות מורשים בלבד ולוודא שגישה באמצעות מפתחות ושילובים פיזיים מנוהלת ומפוקחת באופן קפדני. יש לשמור על נתיב ביקורת עבור מחזיקי הרשאות גישה/מפתחות/שילוב בין השניים, המכסה מקרים של הענקת הרשאות גישה, שינויים בהרשאות הגישה וביטול הרשאות גישה.</p> <p>יש לנהל באופן יעיל את כל הרשאות הגישה כדי לצמצם את הסיכון למקרים של גישה בלתי מורשית. יש לנהל את הרשאות הגישה בהתאם לנהלי בקרת הגישה של הספק. ניתן להנפיק הרשאות גישה ייחודיים רק לאחר קבלת האישור המתאים. יש לתקן את כל הרשאות הגישה לאזורים מוגבלים במרווחי זמן מתאימים. כשאין עוד צורך בגישה למקום או לאזור מוגבל, על הגורם האחראי על ניהול אישורי הגישה להשבית את הרשאות הגישה לא יאוחר מ-24 שעות ממועד קבלת ההודעה מהיחידה העסקית הרלוונטית או ממועד קבלת הודעה בדבר שינויים בדרישות עבור העובד הרלוונטי (כגון, שינוי תפקיד או תחומי אחריות, פיטורין או סיום העסקה).</p>	<p>1. בקרת גישה (TC 5.1)</p>
<p>כדי להגן על נכסים או נתונים של Barclays המאוחסנים במרכזי נתונים, חוות שרתים ומתקנים של ספקים (הן בבעלות הספקים והן בבעלות של צדדים שלישיים כלשהם) מפני אובדן, נזק או גנבה בשל גישה בלתי מורשית לשטח מוגבל.</p>	<p>יש להגדיר וליישם את אמצעי האבטחה הדרושים כדי להגן על אזורים המכילים מידע ונכסים הקשורים אחרים, בהתאם לסביבת הסיכון ולסוג האיום שזוהה או נחזה. יש לתכנן וליישם אבטחה פיזית למשרדים, חדרים ומתקנים (כולל מערכות בקרת גישה, מצלמות אבטחה, מערכות לזיהוי פולשים ואמצעי פיקוח טכניים המתאימים לאבטחה של סביבת אחרות) על בסיס גישה מבוססת סיכונים המסתמכת על רמות האיום הנוכחיות והצפויות ולהתאימה לתהליכים העסקיים המתבצעים וכן למידע המוחזק בנכס ולערך הנכס עצמו.</p> <p>יש לתכנן וליישם תהליכי אבטחה עבור סביבת העבודה באזורים המאובטחים. יש ליישם כללים ברורים לגבי שימוש בנייר ובמדיות</p>	<p>2. אבטחת מרחבים, מבנים וחללים (TC 5.2)</p>

	<p>אחסון ניידות וכללים ברורים לגבי שימוש במסכים עבור מתקנים שבהם מתבצע עיבוד מידע.</p> <p>יש לאבטח באופן יעיל את כל מרכזי הנתונים שהם עצמאיים, משותפים ובבעלות צדדים שלישיים, מרכזי נתונים של ספקי שירותי ענן, חוות שרתים ומרכזי תקשורת (כולל חדרי שרתים וארונות תקשורת עצמאיים) כדי למנוע גישה בלתי מורשית ומקרים של גנבה או נזק לנכסים או לנתונים של Barclays. במתקנים שבהן קיימות התקנות משותפות, יש לפרוס אמצעי אבטחה אפקטיביים המאפשרים ליצור הפרדה יעילה ולקיים שגרת ניטור רציפה</p>	
<p>פריסה והפעלה של בקרות אבטחה פיזיות שתואמות לאיומים הנוכחיים והצפויים תגביל או תמנע את ההשפעה במקרים של גישה בלתי מורשית, גנבה או נזק מכון למתקנים ונכסים.</p>	<p>יש לתכנן מסגרת הגנה מפני איומים פיזיים על תשתיות ונכסים וליישם אותה באמצעות פריסה של מצלמות אבטחה, מערכות זיהוי פולשים ו/או אמצעי פיקוח רב-שכבתיים נוספים המתאימים לסביבה במאוימת. יש ליישם שגרת ניטור רציפה על האתר כדי לזהות גישה פיזית בלתי מורשית.</p> <p>יש להתקין את כל הציוד באופן מאובטח ומוגן. יש להקפיד שכבלי חשמל, כבלים להעברת נתונים וכבלי תקשורת מוגנים מפני גישה פיזית, הפרעות או גרימת נזק. יש לוודא שפעולות ההתקנה והתחזוקה של ציוד האבטחה ומהמערכות מתבצעות בהתאם לדרישות היצרן ולהקפיד על שגרת ניטור על מנת להבטיח זמינות, שלמות וסודיות של המידע.</p> <p>יש להקפיד שהנכסים של Barclays המאוחסנים מחוץ לאתר נותרים מוגנים, הן במעבר והן במנוחה.</p> <p>יש לוודא שפעולות ההתקנה והתחזוקה של הציוד מתבצעות כהלכה ובהתאם לתקני התעשייה כדי להבטיח זמינות, שלמות וסודיות של המידע. יש לוודא שפעולות ההתקנה וההפעלה של כל מערכות האבטחה מתבצעות בהתאם לדרישות החוק והרגולציה החלות.</p> <p>אם קיימים, אזורי אספקה והטעינה חייבים להיות מבוקרים ומבודדים כהלכה מאזורים תפעוליים כדי למנוע גישה בלתי מורשית ואיום פוטנציאלי בשל משלוחים לא מאומתים.</p>	<p>3. הגנה מפני איומים פיזיים על תשתיות ונכסים (TC 5.3)</p>

לאחר זיהוי היקף אמצעי הניהול שיש להחיל, יש לקרוא תקן זה יחד עם התקן הבא:

חובת פיקוח על ספקי שירות שהם צדדים שלישיים (TPSPCO), דרישות בקרת ניהול - מידע, אבטחת סייבר ואבטחה פיזית, טכנולוגיה, תכנון שחזור והתאוששות, פרטיות נתונים, ניהול נתונים, PCI, EUDA ו-DSS.

גרסה 13.0, ספטמבר 2023