المسار الرياضي
Sports Boulevard

دليل إرشادي لإلتزامات الأمن السيبراني للأطراف الخارجية

Cybersecurity Third Party Guidelines

| Content

| المحتويات

2. Terms and Definitions | 2. الاختصارات والتعريفات

2.1 Abbreviations | 1.2 الاختصارات

Term	Description	الوصف	الاختصار
SBF	Sports Boulevard Foundation.	مؤسسة المسار الرياضي	**المؤسسة**

2.2 Definitions | 2.2 التعريفات

Terminology	Description	التعريف	النص
Third Party	A representative of an external organization providing services, products, or support to SBF, who may hold job titles such as Coordinator, Consultant, Specialist, Account Manager, Service Representative, Lead, Senior Lead, or Expert.	ممثل لجهة خارجية أو مورد يقدم خدمات أو منتجات أو دعماً لمؤسسة المسار الرياضي، وقد يحمل أحد المسميات الوظيفية مثل: منسق، استشاري، أخصائي، مدير حسابات، ممثل خدمات، قائد فريق، قائد أول، أو خبير.	**الأطراف الخارجية**

3. Purpose | 3. الهدف

The purpose of this Guideline is to set forth the minimum Cybersecurity requirements for Sports Boulevard Foundation Third Parties to protect SBF from possible cyber threats and strengthen Third Parties' security posture.

الغرض من هذا الدليل هو وضع الحد الأدنى من متطلبات الأمن السيبراني لمزودي الخدمة والأطراف الخارجية الخاصة بـ مؤسسة المسار الرياضي وذلك لحماية المؤسسة من التهديدات السيبرانية المحتملة، وتعزيز الوضع الأمني لهذه الأطراف .

4. Scope | 4. النطاق

This Guideline applies to All Third Parties engaging with Sports Boulevard Foundation through contractual agreements.
Additional specific cybersecurity requirements are defined for a Third Party who is classified as "Major" and "Catastrophic.

يطبق هذا الدليل على كافة الجهات المتعاقدة مع مؤسسة المسار الرياضي. سيتم تطبيق ضوابط إضافية وأكثر تفصيلاً على الأطراف المصنفة ضمن فئات المخاطر (عالية) أو (كارثية) وفقاً لمعايير التقييم الخاصة بالمؤسسة.

5. Ownership & Review | 5. الملكية والمراجعات

5.1 The Cybersecurity Department shall have the responsibility for preparing and the custody over the master copy of this Guideline and reviewing it every year or when there are regulatory or organizational changes that affect the Foundation or the context within which the Foundation operates or when the need to make changes arise. To ensure

1.5 تتولى إدارة الأمن السيبراني مسؤولية إعداد النسخة الرئيسية من هذا الدليل والاحتفاظ بها ومراجعتها كل سنة، أو عندما تكون هناك تغييرات في الأنظمة والتشريعات، أو أية تغيرات تنظيمية تؤثر على المؤسسة أو السياق الذي تعمل فيه المؤسسة، أو عندما تنشأ الحاجة إلى إجراء تغييرات، للتأكد من أن هذه الوثيقة متوافقة وكافية مع

that this Guideline aligned and adequate to applicable laws, regulations, SBF organizational structure and policies, and international standards.

الأنظمة والتشريعات وهيكل المؤسسة التنظيمي وسياساتها والمعايير الدولية.

5.2 This Guideline is subject to the (Cybersecurity Governance, Risk and Compliance Chief) approval

2.5 يخضع هذا الدليل لموافقة لرئيس قطاع الحوكمة ,والمخاطر والالتزام

6. References and Supporting Documents

6. المراجع والوثائق الداعمة

6.1 NCA (National Cybersecurity Authority) Controls

6.1 ضوابط الهيئة الوطنية للأمن السيبراني (NCA)

7. The Guideline Statement

7. بيان الدليل الاسترشادي

7.1 General Provision

7.1 أحكام عامة

Control Name	Network connectivity	Managed Services	Software development	Cloud Services
Asset Management				**إدارة الأصول**
Third Party must have policies and procedures to classify information in terms of its criticality يجب أن يتوفر لدى الأطراف الخارجية سياسات وإجراءات للتعامل مع البيانات وتصنيفها بناءً على درجة أهميتها وحساسيتها.	√	√	√	√
Governance				**الحوكمة**
Third Party must be staffed by employee(s) whose primary responsibility is Cybersecurity. يجب على يكون لدى الأطراف الخارجية موظف (موظفون) مسؤولين عن الأمن السيبراني.	√	√		
Third Party must have formal procedures for on-boarding employees that include background checks. يجب على الاطراف الخارجية وضع إجراءات رسمية لتعيين الموظفين ويجب أن تتضمن هذه الإجراءات إجراء مسح أمني.	√	√	√	√
Risk Assessment, Vulnerability Management and Penetration Testing				**إدارة المخاطر, إدارة الثغرات و اختبار الاختراق**
Third Party must have a process to conduct Cybersecurity Risk Assessment on a regular basis, to identify, assess and remediate Risks to data and information systems. يجب على الأطراف الخارجية إجراء تقييم مخاطر الأمن السيبراني بشكل منتظم، وذلك لتحديد وتقييم ومعالجة المخاطر التي تهدد البيانات وأنظمة المعلومات.	√	√		

Third Party must conduct annual external Penetration Testing on its IT infrastructure systems, and internet facing applications. يجب على الأطراف الخارجية إجراء اختبارات الاختراق بشكل دوري على بنية تقنية المعلومات التحتية، والأنظمة، والتطبيقات المتصلة بالإنترنت.	√	√	√	√
Monthly Vulnerability scans must be conducted to evaluate configuration, Patches and services for known Vulnerabilities. يجب إجراء عمليات فحص شهرية للثغرات الأمنية بحثًا عن الثغرات الأمنية المعروفة.	√	√	√	√
Network Security	**أمن الشبكات**			
Network connections to information systems and applications at the Third Parties location must be authorized and monitored. يجب أن تكون اتصالات الشبكة الخاصة بأنظمة المعلومات والتطبيقات في الأطراف الخارجية مصرح بها وخاضعة للمراقبة.	√	√		√
Multi-factor authentication must be enforced on all privileged accounts of access, including remote access to information systems and applications. يجب على الأطراف الخارجية فرض التحقق متعدد العناصر على جميع عمليات الوصول للحسابات ذات الصلاحيات العالية، بما في ذلك الوصول عن بعد إلى أنظمة المعلومات والتطبيقات.	√	√	√	√
Third Party must encrypt data in transit (e.g. SSH, FTPS, HTTPS, TLS, IPSEC). يجب على الأطراف الخارجية تشفير البيانات أثناء النقل مثل: SSH، FTPS، HTTPS، TLS، IPSEC		√	√	√
Third Party must implement encryption mechanisms, using at least AES encryption algorithm, and 256 bit key, on all devices or storage media hosting sensitive data per the Third Party's assets classification policy. يجب على الاطراف الخارجية تنفيذ آليات التشفير باستخدام خوارزمية تشفير لا تقل عن AES وبمفتاح بطول 256 بت، وذلك على جميع الأجهزة أو وسائط التخزين التي تستضيف بيانات حساسة، وفقًا لسياسة تصنيف الأصول الخاصة بالاطراف الخارجية.	√	√		√
Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) must be implemented at the network perimeter. يجب تطبيق أنظمة كشف التسلل أو أنظمة منع التسلل على محيط الشبكة.	√	√	√	√
Information Processes and Procedures (IP)	**عمليات وإجراءات حماية المعلومات**			
Third Party must establish and follow regular procedures for backup of critical systems and Sports Boulevard Foundation's data, software and websites. يجب على الاطراف الخارجية وضع واتباع إجراءات للنسخ الاحتياطي للأنظمة الحساسة، وبيانات وبرمجيات ومواقع مؤسسة المسار الرياضي و اختبار استعادة النسخ الاحتياطي	√	√	√	√

Third Party must have a process for secure system and software development life cycle in alignment with industry best practice. يجب على الاطراف الخارجية اعتماد عملية آمنة لدورة حياة تطوير الأنظمة والبرمجيات، بما يتوافق مع أفضل الممارسات المتبعة في الصناعة.			√	√
Logging & Monitoring	**سجلات الأحداث ومراقبة الأمن السيبراني**			
Third Party must retain all audit logs from information systems and applications for storing, processing or transmitting SBF data for one (1) year. يجب على الاطراف الخارجية الاحتفاظ بجميع سجلات التدقيق من أنظمة المعلومات والتطبيقات التي تخزن أو تعالج أو تنقل بيانات مؤسسة المسار الرياضي لمدة عام واحد (1).	√	√	√	√
Third Party must monitor Technology Assets, Systems and applications to identify unauthorized access, or unauthorized activity. يجب على الاطراف الخارجية مراقبة الأصول التقنية والأنظمة والتطبيقات لتحديد الوصول غير المصرح به أو النشاط غير المصرح به.	√	√		√
Privileged accounts activity must be logged and monitored on a regular basis. يجب تسجيل ومراقبة أنشطة الحسابات ذات الصلاحيات العالية بشكل منتظم.	√	√	√	√
Business Continuity & Incident Management	**استمرارية الأعمال وإدارة الحوادث**			
Incident management policy and plan must be documented, maintained and communicated to management and appropriate team members. يجب توثيق سياسة وخطة إدارة الحوادث، والاحتفاظ بها، وإبلاغها للإدارة وأعضاء الفريق المعنيين.	√	√	√	√
Third Party must have a Disaster Recovery Plan (DR Plan) which is documented, maintained and communicated to appropriate parties. The DR Plan should address the recovery of Assets and communications following a major disruption to business operations. يجب على الاطراف الخارجية إعداد خطة للتعافي من الكوارث تكون موثقة ومحدثة ويتم إبلاغ الأطراف المعنية بها. كما ينبغي أن تحتوي على خطة التعافي استعادة الأصول ووسائل الاتصال بعد حدوث كوارث في العمليات التشغيلية.	√	√	√	√
Third Party must have a comprehensive Business Continuity (BC) plan which is documented, maintained and communicated to appropriate parties. يجب على الاطراف الخارجية إعداد خطة شاملة لاستمرارية الأعمال تكون موثقة ومحدثة ويتم إبلاغها إلى الأطراف المعنية.	√	√	√	√
Third Party must conduct Business Continuity drills at least annually. إجراء اختبارات لاستمرارية الأعمال مرة يجب على الاطراف الخارجية واحدة على الأقل سنويًا	√	√	√	

8. Appendices

8. المرفقات

N/A

لا يوجد