SunExpress

SUNEXPRESS GÜNEŞ EKSPRES HAVACILIK A.Ş.

Information Security Policy

1. Introduction

SunExpress takes information security seriously and is committed to providing assurance to its people and to customers, business partners and other third parties that information is managed in a controlled and secure environment.

This document sets out the Information Security Policy (ISP) for SunExpress.

Information shall mean any content whatever its medium (whether written on paper or stored in any form electronic, hardcopy or otherwise including but not limited to sound, visual or audio-visual recordings). Information security in the context of this policy means the preservation of confidentiality and integrity of information and prevention of unauthorised disclosure of Information.

2. Purpose

This policy supplements and reinforces other SunExpress policies, practices and procedures connected to information and cyber security. In association with security standards, this policy consolidates legal, regulatory and company obligations into a set of objectives and requirements that enable a robust control environment to be implemented.

3. Scope

This policy applies across the company to all colleagues and third parties working on behalf of SunExpress with access to SunExpress applications, infrastructure, and information.

4. Management Statement

The security of information, computing infrastructure and systems including applications is vital to maintaining our reputation and ability to achieve our business objectives.

Management is committed to ensuring that SunExpress business obligations including contractual, legal, and regulatory requirements are always met. The protection of company information and business assets is the responsibility of everybody including business partners and third parties.

4.1 Management Intent

It is the intent of management that:

- Assets of the company are adequately protected.
- Regulatory and legislative requirements are met at all times.
- Control measures are implemented that are commensurate with risk.
- Business continuity plans are available, maintained and tested.

4.2 Information Security Requirement

This policy requires that:

- All applications, infrastructure, information, and suppliers are classified in a way that indicates its importance to the company.
- Owners are appointed for all applications, infrastructure, classified information, and supplier relationships.
- Owners of applications, infrastructure, classified information, and supplier relationships **must** ensure they are risk assessed on agreed basis or before a significant change.
- All information assets are protected in terms of their requirements for confidentiality, integrity and availability following an approved process for identifying and managing risks.
- Individuals using or accessing SunExpress information assets or resources are made aware of their security responsibilities.

4.3 Incident Reporting

All security policy, standards or framework breaches must be reported promptly to SunExpress Information Security using the following email address info.sec@sunexpress.com.

5. Policy Restrictions

It is expressly prohibited to:

- Alter or tamper with security evidence or log sources.

6. Policy Compliance

6.1 Compliance Measurement

The SunExpress Information Security team will verify compliance with this policy through various methods, including but not limited to, security and/or business tool reports, internal and external audits, and shall provide feedback to the policy owner.

6.2 Exceptions

Any exceptions or non-conformance with SunExpress information security policy or standards **must** be approved in advance by Information Security following a documented process for tracking and reporting on all exceptions and non-conformance.

6.3 Non-Compliance

Colleagues violating this policy or supporting policies (including acceptable use policies) may be subject to disciplinary action, up to and including termination of employment.

7. Responsibilities

The following roles are in place within SunExpress to assist in the provision of sound information security practice across the company.

- Information & Cyber Security Senior Manager, Ayo Adebayo – Responsible for the overall coordination of Information Security, including security improvement, security training and awareness and the maintenance of this policy.
- IT Director, Mustafa Egilmezbilek – Owner of the SunExpress Information Security Policy and executive sponsor for information and cyber security in the company.

Signed

Max Kownatzki
CEO

Tuncay Eminoğlu
Deputy CEO

SunExpress

SUNEXPRESS GÜNEŞ EKSPRES HAVACILIK A.Ş.

Bilgi Güvenliği Politikası

1. Giriş

SunExpress bilgi güvenliğini ciddiyetle ele almaktadır ve çalışanlarına, müşterilerine, iş ortaklarına ve diğer üçüncü taraflara bilgilerin kontrollü ve güvenli bir ortamda yönetildiğine dair güvence vermeyi taahhüt eder.

Bu doküman, SunExpress Bilgi Güvenliği Politikası'nı (BGP) ortaya koymaktadır.

Bilgi, hangi ortamda olursa olsun (kağıt üzerinde yazılı veya herhangi bir biçimde elektronik, basılı kopya veya sesli, görsel veya görsel-işitsel kayıtlar dâhil ancak bunlarla sınırlı olmamak üzere sair biçimlerde saklanan) her türlü içeriği ifade eder. Bu politika metni bağlamında bilgi güvenliği, bilgilerin gizliliğinin ve bütünlüğünün korunmasını ve bilgilerin izinsiz bir şekilde ifşasının önlenmesini ifade eder.

2. Amaç

Bu politika metni, bilgi ve siber güvenlikle bağlantılı diğer SunExpress politikalarını, uygulamalarını ve prosedürlerini tamamlayıcı ve pekiştirici niteliktedir. Güvenlik standartları açısından değerlendirildiğinde bu politika metni; hukuki, düzenleyici ve kurumsal yükümlülükleri, sağlam bir kontrol ortamının uygulanmasına olanak sağlayan bir hedef ve gereklilikler grubu içinde birleştirir.

3. Kapsam

Bu politika, şirket genelinde SunExpress uygulamalarına, altyapısına ve bilgilerine erişimi olan ve SunExpress adına görev yapan tüm çalışanlar ve üçüncü taraflar için geçerlidir.

4. Yönetim Beyanı

Bilgilerin, bilişim altyapısının ve uygulamalar dâhil olmak üzere sistemlerin güvenliği, itibarımızın ve iş hedeflerimize ulaşma kabiliyetimizin sürdürülmesi açısından çok önemlidir.

Yönetim; akdi, hukuki ve düzenleyici gereklilikler dâhil olmak üzere, SunExpress iş yükümlülüklerinin her zaman yerine getirilmesini sağlamayı taahhüt eder. Şirket bilgilerinin ve iş varlıklarının korunmasından, iş ortakları ve üçüncü taraflar dâhil herkes sorumludur.

4.1 Yönetimin Gayesi

Yönetimin ulaşmak istediği gayeler şunlardır:

- Şirket varlıklarının yeterli düzeyde korunması.
- Düzenleyici ve yasal gerekliliklerin her zaman yerine getirilmesi.
- Kontrol önlemlerinin riskle orantılı bir biçimde uygulanması.
- İş sürekliliği planlarının mevcut olması, idame ve test edilmesi.

4.2 Bilgi Güvenliği Gerekliliği

Bu politika şu hususları gerekli kılmıştır:

- Tüm uygulamaların, altyapının, bilgilerin ve tedarikçilerin, şirket açısından önemini ortaya koyacak şekilde sınıflandırılması.
- Tüm uygulamalar, altyapı, gizlilik dereceli bilgiler ve tedarikçi ilişkilerinden sorumlu kişilerin/birimlerin atanması.
- Uygulamalar, altyapı, gizlilik dereceli bilgiler ve tedarikçi ilişkilerinden sorumlu olan kişilerin/birimlerin, üzerinde mutabık kalındığı şekilde veya kayda değer bir değişiklik öncesinde risk değerlendirmesi yapılmasını sağlamak **zorunda olması**.
- Tüm bilgi varlıklarının, risk tespiti ve yönetimi için onaylanmış bir süreç uygulanmak suretiyle gizlilik, bütünlük ve kullanılabilirlik gereklilikleri açısından korunması.
- SunExpress bilgi varlıklarını veya kaynaklarını kullanan veya bunlara erişim sağlayan kişilerin, güvenlik sorumlulukları konusunda bilgilendirilmesi.

4.3 Olay Bildirimi

Güvenlik politikasına, standartlarına veya çerçevesine yönelik tüm ihlaller, info.sec@sunexpress.com e-posta adresi üzerinden derhal SunExpress Bilgi Güvenliği ekibine bildirilmelidir.

5. Politika Kısıtlamaları

Bu politika metni kapsamında yasaklanan işlemler:

- Güvenlik kanıtlarının veya denetim izlerinin değiştirilmesi veya bozulması.

6. Politikaya Uyum

6.1 Uyum Ölçümü

SunExpress Bilgi Güvenliği ekibi, güvenlik ve/veya iş raporları, iç ve dış denetimler dâhil ancak bunlarla sınırlı olmamak üzere çeşitli yöntemlerle bu politikaya uyumu doğrulayacak ve politika sorumlusuna geri bildirimde bulunacaktır.

6.2 İstisnalar

SunExpress bilgi güvenliği politikası veya standartları kapsamındaki istisnalar veya uyumsuzluklar, tüm istisnalar ve uygunsuzlukların izlenmesi ve bildirilmesine yönelik yazılı süreç uygulandıktan sonra Bilgi Güvenliği ekibi tarafından önceden **onaylanmalıdır**.

6.3 Uygunsuzluk

Bu politikayı veya destekleyici politikaları (kabul edilebilir kullanım politikaları dâhil) ihlal eden çalışanlara, iş akdinin feshine varan disiplin cezaları uygulanabilir.

7. Sorumluluklar

Şirket genelinde güçlü bir bilgi güvenliği uygulamasının sağlanmasına yardımcı olmak adına SunExpress bünyesinde aşağıdaki atamalar yapılmıştır.

- Bilgi ve Siber Güvenlik Grup Müdürü, Ayo Adebayo – Güvenlik geliştirme, güvenlik eğitimi ve farkındalığı ile bu politikanın sürdürülmesi dâhil olmak üzere Bilgi Güvenliği eylemlerinin genel koordinasyonundan sorumludur.
- BT Direktörü Mustafa Eğilmezbilek – SunExpress Bilgi Güvenliği Politikası'ndan sorumludur ve şirketin bilgi ve siber güvenlik uygulamalarını idari olarak destekler.

İmza

Max Kownatzki
CEO

Tuncay Eminoğlu
CEO Yardımcısı

Confirmation Code: xvqaC3