BİLGİ GÜVENLİĞİ POLİTİKASI
INFORMATION SECURITY POLICY

PL.ITM.10.001 Rev. 03

TUSAŞ'a ait bilgi varlıklarının gizlilik, bütünlük ve ulaşılabilirliğinin sağlanması, yasal gerekliliklerin yerine getirilmesi ve TUSAŞ paydaşlarının bilgi güvenliği ve siber güvenlik konularındaki farkındalığının arttırılması için; bilgi güvenliği ve siber güvenlik konularında yetkin insan kaynağı ve sürekli iyileştirme yaklaşımıyla gerekli teknolojik çözümlerin ve süreçlerin tesis edilerek işletilmesidir.

To ensure the confidentiality, integrity, and availability of Turkish Aerospace's information assets, to meet legal requirements, and to enhance the awareness of Turkish Aerospace stakeholders regarding information security and cybersecurity, the necessary technological solutions and processes are established and operated by competent human resources through a continuous improvement approach in the areas of information security and cybersecurity.

- TUSAŞ Yönetimi, TUSAŞ'ın stratejileriyle uyumlu olacak şekilde bilgi güvenliği ve siber güvenlik prensipleri ve amaçlarına uygun politikalar, hedefler, usuller ve kuralların belirlenmesini, dokümante edilmesini, siber tehditler ve değişen ihtiyaçlara uygun olarak güncellenmesini ve tüm iş süreçlerinde etkin şekilde uygulanması için geliştirilen düzenlemelerin ilgili tüm TUSAŞ paydaşlarına (işgören, danışman, ziyaretçi, alt yüklenici, iş ortağı vb.) açık ve anlaşılır şekilde duyurulmasından sorumludur.

  Turkish Aerospace Management is responsible for defining, documenting, and updating— in line with Turkish Aerospace's strategies— the policies, objectives, procedures, and rules that comply with information security and cybersecurity principles and goals; ensuring that they are updated in accordance with cyber threats and changing needs, and that the developed arrangements are communicated to all relevant Turkish Aerospace stakeholders (employees, consultants, visitors, subcontractors, business partners, etc.) in a clear and understandable manner for effective implementation throughout all business processes.

- TUSAŞ'ta kurulan Bilgi Güvenliği Yönetim Sistemi (BGYS), ISO/IEC 27001 standardı ve EASA PART IS düzenlemelerinin gerekliliklerine uyumludur ve bu uyumluluk, düzenli olarak yapılan iç ve dış denetimlerle belgelendirilir.

  The Information Security Management System (ISMS) established at Turkish Aerospace complies with the requirements of ISO/IEC 27001 standard and EASA PART IS regulations, and this compliance is verified through regular internal and external audits.

- TUSAŞ Yönetimi, işletilen BGYS'nin performansını yönetim gözden geçirmesi kapsamında periyodik olarak değerlendirir, iyileştirilerek sürdürülmesini, en güncel ve uygulanabilir teknolojiler takip edilerek geliştirilmesini temin eder.

  The Turkish Aerospace Management periodically evaluates the performance of the ISMS within the scope of management review, ensures its improvement and continuity, and promotes its development by following the most up-to-date and applicable technologies.

- BGYS hedefleri, TUSAŞ Stratejik Planı ve Bilgi Güvenliği Politikası ile uyumlu ve ölçülebilir olacak şekilde, risk değerlendirme ve iyileştirme çalışmalarından beslenerek ve bilgi güvenliği gereksinimleri ve şirket kaynakları göz önüne alınarak belirlenir.

  ISMS objectives are determined in alignment with Turkish Aerospace's strategic plan and information security policy, in a measurable manner, based on risk assessment and improvement activities, while taking into account information security requirements and corporate resources.

- TUSAŞ Yönetimi, bilgi güvenliği risklerinin etkin bir şekilde yönetilmesi (bilgi güvenliği ile ilgili risklerinin belirlenmesi, bu risklerin havacılık emniyetiyle ilgili olanların belirlenmesi, risk değerlendirmenin yapılması, uygun risk işleme yönteminin seçilmesi ve seçilen risk işleme yöntemine uygun olarak gerekli aksiyonların uygulamaya konulması) ve süreçlerin tesis edilerek işletilmesini sağlatmaktan sorumludur.

  The Turkish Aerospace Management is responsible for ensuring the effective management of information security risks (identifying risks related to information security, determining those linked to aviation safety, performing risk assessment, selecting appropriate risk treatment methods, and implementing the necessary actions in accordance with the selected method) and for establishing and operating related processes.

- TUSAŞ Yönetimi, belirlenen kritik süreçlerde bilgi sistemleri problemleriyle olağanüstü durumlarda sistemin olası bir kesintiye uğraması (süreli olarak hizmet dışı kalması) durumunda, sürecin en kısa sürede yeniden işlerliğini sağlayacak ya da ikame edilecek acil durum işlemlerinin belirlendiği İş Sürekliliği Planlarının hazırlanmasını ve uygulanmasını temin eder.

  The Turkish Aerospace Management ensures that Business Continuity Plans are prepared and implemented for critical processes to define emergency actions that will either restore operations in the shortest possible time or provide alternatives in case of possible interruptions (temporary service outages) of the system due to information system problems or extraordinary situations.

- TUSAŞ, bilgi güvenliği konusunda farkındalık düzeyinin arttırılması amacıyla ilgili tüm paydaşların gerekli eğitimleri almalarını sağlar.

  Turkish Aerospace ensures that all relevant stakeholders receive the necessary training to increase awareness levels regarding information security.

- Bilginin gizliliği, bütünlüğü, doğruluğu ve ulaşılabilirliğinin korunması karlılık, nakit akışı, yasal yükümlülüklerin devamlılığı için zaruridir. TUSAŞ'ın tüm paydaşları bilgi güvenliği ile ilgili yürürlükteki TUSAŞ'ı bağlayan yasa ve mevzuata, TUSAŞ'ın yapmakta olduğu iş ve sözleşmeler gereği doğan yükümlülüklere ve kendilerine aktarılan veya referans olarak iletilen TUSAŞ tarafından hazırlanan kurumsal dokümanlardaki usullere uymak zorundadır.

  Protecting the confidentiality, integrity, accuracy, and availability of information is essential for profitability, cash flow, and the continuity of legal obligations. All Turkish Aerospace stakeholders are required to comply with applicable laws and regulations binding Turkish Aerospace, obligations arising from Turkish Aerospace's activities and contracts, and the procedures specified in corporate documents prepared or referenced by Turkish Aerospace.

- TUSAŞ paydaşlarının, TUSAŞ tesislerinde ya da dışında bulunan bilgi sistemleri aracılığıyla işleri gereği eriştikleri TUSAŞ'a ait bilgiler için yetkilendirme, "Bilmesi Gereken Prensibi" çerçevesinde sağlanır, erişimler kayıt altına alınır ve verilen yetkiler düzenli olarak gözden geçirilir.

  Authorization for access to Turkish Aerospace's information, accessed by stakeholders through information systems located inside or outside Turkish Aerospace premises, is granted based on the "Need to Know Principle"; all accesses are logged, and granted privileges are regularly reviewed.

- TUSAŞ Bilgi Teknolojileri (BT) kaynakları, ilgili onaylar ve yetkiler alındıktan sonra sadece TUSAŞ işleri için kullanılabilir. TUSAŞ BT kaynaklarına erişim sırasında görüntülenen güvenlik uyarı mesajları bağlayıcıdır.

  Turkish Aerospace Information Technology (IT) resources may only be used for Turkish Aerospace business purposes after obtaining the necessary approvals and authorizations. Security warning messages displayed during access to Turkish Aerospace IT resources are binding.

- TUSAŞ yerel ağında kullanılan kurumsal BT kaynaklarının TUSAŞ tüzel kimliğine ait olarak tahsis edilen lisanslı yazılım / donanımlar olması sağlanır. Meşru olmayan (korsan) yazılımların kullanımına izin verilmez. Kopya hakkı ile korunmakta olan yazılımlar, kopyalama hakkı sahibinin ya da temsilcisinin izni olmadan kullanılamaz ve kopyalanamaz.

  IT resources used within the Turkish Aerospace local network must consist of licensed software/hardware allocated under Turkish Aerospace's legal entity. The use of illegitimate (pirated) software is not permitted. Software protected by copyright cannot be used or copied without the permission of the copyright holder or its authorized representative.

- TUSAŞ, 5846 sayılı Fikir ve Sanat Eserleri Kanunu'na göre fikrî mülkiyet kapsamına giren varlıkların (yazılım ve doküman kopya hakkı, tasarım hakkı, tescilli marka, patent ve yazılım kaynak kod lisanslarıyla korunan bilgiler) ilgili yasa, yönetmelik ve sözleşmelerin hükümlerine uygun olarak korunmasını temin etmek üzere gerekli önlemleri alır.

  In accordance with Law No. 5846 on Intellectual and Artistic Works, Turkish Aerospace takes necessary measures to ensure that assets falling under the scope of intellectual property (software and document copyrights, design rights, registered trademarks, patents, and software source code licenses) are protected in compliance with relevant laws, regulations, and contractual provisions.

- 5202 sayılı Savunma Sanayii Güvenliği Kanunu hükümleri doğrultusunda TUSAŞ'ta gizlilik dereceli bilgi, belge ve malzemeye nüfuz etmesi muhtemel tüm personel için (danışmanlar dahil) Millî Savunma Bakanlığı'ndan Kişi Güvenlik Belgesi alınır.

  In line with the provisions of the Defense Industry Security Law No. 5202, Turkish Aerospace obtains a Personal Security Clearance Certificate from the Ministry of National Defense for all personnel (including consultants) who may have access to classified information, documents, and materials.

- Gizlilik dereceli bilgi, belge ve malzeme; hizmet gereği bilmesi gereken ve uygun gizlilik dereceli kişi / tesis güvenlik belgesi bulunan kişi ve kuruluşlara verilir. Bu maksatla gizlilik dereceli bilgi paylaşımının söz konusu olacağı alt yüklenici süreçlerinde, potansiyel alt yüklenici personelinin Kişi Güvenlik Belgesi ve tesisinin Tesis Güvenlik Belgesi sahibi olduğu doğrulanır. Gizlilik dereceli bilgilere yetkisiz erişimi önlemek üzere, bu bilgilerin muhafazası veya transferi sırasında kriptolama tekniklerinin kullanılması sağlanır.

  Classified information, documents, and materials are provided only to individuals or organizations who have the need to know for service purposes and hold an appropriate level of personal or facility security clearance. In subcontractor processes where classified information

sharing will occur, it is verified that potential subcontractor personnel possess a Personal Security Clearance Certificate and that their facilities hold a Facility Security Clearance Certificate. Encryption techniques are used during the storage or transfer of classified information to prevent unauthorized access.

- TUSAŞ bilgi sistemlerine veya bilgi işleme araçlarına ürün veya hizmet sağlama yoluyla erişecek ve TUSAŞ'a ait bilgiye nüfuz edecek Üçüncü Taraflarla yapılan sözleşmelerde bilgi güvenliğiyle ilgili gereksinimlerinin yer alması sağlanır ve standart "Bilgi Değişimi ve Gizlilik Sözleşmesi" imzalanır.

  Contracts signed with Third Parties that will access Turkish Aerospace's information systems or gain access to Turkish Aerospace's information through the supply of products or services include information security requirements, and a standard "Information Exchange and Confidentiality Agreement" is signed.

- TUSAŞ bilgi sistemlerine bağlantı sağlayacak bilgisayar kullanıcılarına, Kullanıcı Gizlilik Taahhütnamesi imzalatılır.

  Computer users who will connect to Turkish Aerospace information systems are required to sign a User Confidentiality Undertaking.

- Tüm TUSAŞ çalışanları, bilgi güvenliği açısından tehlike oluşturabilecek olası durumları önceden tespit etmeye çalışır ve gerçekleşen güvenlik ihlalleri için ilgili usullere göre bildirimde bulunur. Güvenlik ihlali durumunda olay değerlendirilir, ilgili yönergeler ve yasalar doğrultusunda gerekli işlemler yapılır. TUSAŞ yönetimi, bilgi güvenliği olaylarının tekrarını önlemek için caydırıcı önlemler almaktan sorumludur.

  All Turkish Aerospace employees are expected to identify potential situations that may pose a risk to information security in advance and report any security incidents in accordance with relevant procedures. In case of a security incident, the event is evaluated, and necessary actions are taken in line with relevant directives and legal requirements. The Turkish Aerospace Management is responsible for implementing deterrent measures to prevent recurrence of information security incidents.

- TUSAŞ paydaşlarının iş amacıyla saklanan veya işlem gören kişisel bilgileri, 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri doğrultusunda korunur.

  Personal data of Turkish Aerospace stakeholders stored or processed for business purposes are protected in accordance with the provisions of the Personal Data Protection Law No. 6698.

- TUSAŞ, internet ortamında tusas.com alan adı üzerinden yayımladığı içerik ve TUSAŞ'ta tanımlı ve internete erişim yetkisi olan bilgisayar kullanıcılarına sağladığı internet erişimi hizmetiyle ilgili 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun hükümlerine uyumluluğun sağlanmasını temin etmek üzere gerekli önlemleri alır.

  Turkish Aerospace takes necessary measures to ensure compliance with the provisions of Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications regarding the content published under the tusas.com domain name and the internet access services provided to authorized users within Turkish Aerospace.

- TUSAŞ, bilgi sistemlerinin gizlilik, bütünlük ve ulaşılabilirliğini olumsuz etkileyecek iç ve dış tehditlere, siber saldırılara, şüpheli yazılım ve zararlı içeriklere karşı gerekli önlemleri alır. Bilgi sistemlerinin güvenlik taramasının yapılması, olası zafiyetlerin tespit edilmesi ve kapatılması, siber olayların teşhisi ve müdahalesi için en uygun teknolojik çözümlerden faydalanır, güvenlik konusunda gerekli yeterliliğe sahip ve yetkin uzmanların istihdamını sağlar. Güvenli bir dijital ortamın oluşturulmasına yönelik bir yaklaşım benimser.

  Turkish Aerospace takes necessary measures against internal and external threats, cyberattacks, suspicious software, and malicious content that may negatively affect the confidentiality, integrity, and availability of information systems. It utilizes the most suitable technological solutions for performing security scans, identifying and remediating vulnerabilities, detecting and responding to cyber incidents, and ensures the employment of adequately qualified and competent experts in the field of cybersecurity. A proactive approach is adopted to create a secure digital environment.

Yönetim Kurulu

Board of Directors