AWARENESS & TRAINING DOCUMENT

VERI GUVENLIGI POLITIKASI

DATA SECURITY POLICY

Document Number	**HSF-TrainingE13**	**First Release Date**	**02.01.2025**	**Does Not Contain ITAR Controlled Data**	
Revision Number	**01**	**Revision Date**	**30.07.2025**	**Cancelled Revision**	**01**

0. GIRIS

0.1. Bu egitim dokumani HSF KYS kapsaminda dahili ve harici sureclerin planlanmasi, uygulanmasi, kontrolu esnasindaki veri guvenliginin nasil uygulanacagini ve kisisel sorumluluklarin sinirlarini belirlemek amaciyla hazirlanmistir.

0.2. Kullanici (Uygulayici) Seviyesi: Bu belgenin kullanici seviyesi tum HSF ailesidir.

0.3. Uygulayici Sorumlulugu: HSF Veri Guvenligi (**DS**) politikasi, HSF bunyesinde calisan tum kisiler icin yer ve konum sinirlamasi olmaksizin 7 gun 24 saat gecerlidir.

0.4. Risk Degeri: HSF DS politikasinin risk degeri surec veya proje kapsamina bakilmaksizin Cok Yuksek siddet ve Cok Yuksek olasilik olarak degerlendirilir.

0. INSTRUCTIONS

0.1. *This training document has been prepared to determine how to implement data security and the limits of personal responsibilities during the planning, implementation, and control of internal and external processes within the scope of the HSF QMS.*

0.2. User (Implementer) Level: *The user level for this document is the entire HSF family.*

0.3. Implementer Responsibility: *The HSF Data Security (DS) policy is valid 24 hours a day, 7 days a week, for all employees working within HSF, regardless of location.*

0.4. Risk Value: *The risk value of the HSF DS policy is evaluated as Very High severity and Very High probability, regardless of the process or project scope.*

1. TUM PERSONELE

1.1. Bu dokumani basdan sona kisisel ve sosyal sorumluluklarinizi ogrenmek icin dikkatlice okuyun ve onaylayin

1.2. Dokuman hakkinda veya sorumluluklariniz hakkinda herhangi bir anlasilmama ve ek bilgiye ihtiyac duyarsaniz lutfen HSF ust yonetimi ile iletisim kurun,

HSF Savunma Havacilik (HSF), bu dokumanin sirket icinde yayinlanmasini ve tum personele ulasmasini, bu belgenin tum personel tarafindan okunup anlasilmis oldugunu kabul eder. Sirket icinde yayinlanan farkindalik egitim dokumanlarinin personel tarafindan anlasilip kabul edildiginin teyidi icin personel imzasina gerek yoktur.

1. TO ALL STAFF

1.1. *Please carefully read and approve this document thoroughly to learn about your personal and social responsibilities.*

1.2. *If you have any questions about this document, your responsibilities, or need additional information, please contact HSF senior management.*

HSF considers the publication of this document within the company and its distribution to all personnel to be deemed read and understood by all personnel. A staff signature is not required to confirm that the awareness training documents published within the company have been understood and accepted by the personnel.

2. VERI GUVENLIGI KURALLARI

2.1. HSF ailesi uyesi olarak, bilgileri musterilerin gecerli gerekliliklerine, yasal duzenlemelere ve HSF'nin bilgi güvenligi gerekliliklerine uygun olarak koruma sorumlulugunuz bulunmaktadir.

2.2. HSF bilgi islem veya bilgi kaynaklarina erisimi olan her birey, ilgili bilgi koruma gerekliliklerine uymali, HSF kaynaklarinin butunlugunu korumali ve bunlari yetkisiz erisime ve dagitimina karsi korumalidir.

2.3. HSF bilgi islem ve bilgi kaynaklarina erisim yalnizca yetkili kisilere verilir ve yalnizca is fonksiyonu, bilme gereksinimi, istihdam durumu ve yonetim onayi temelinde gerekli olanla sinirlidir.

2.4. HSF bilgi islem ve bilgi kaynaklari HSF'nin ticari faaliyetleri icin kullanılabilir ve baska hicbir amacla kullanilamaz.

2.5. Tum HSF personeli asagidaki bilgi ve veri koruma alanlarina uymalidir:

2.6. Bilgi ve Veri Koruma Alanlari

BU KISIM VERI VEYA BELGENIN IZINSIZ KOPYALANMASI, IZINSIZ PAYLASILMASI, IZINSIZ YENIDEN URETILMESI, IZINSIZ KONUSULMASI VE/VEYA KOTULEME AMACLI HERTURLU DAVRANISI KAPSAR VE BUNLARDAN HERHANGI BIRI VEYA HEPSI KOSULSUZ IS AKDI FESHI ANLAMINA GELIR.

2. DATA SECURITY RULES

2.1. *As a staff member of HSF, you have a responsibility to safeguard the information in accordance with applicable requirements of the customers, legal regulations, as well as HSF's information security requirements.*

2.2. *Every individual with access to HSF computing or information resources must follow relevant information protection requirements, maintain the integrity of HSF resources, and protect them from unauthorized access.*

2.3. *Access to HSF computing and information resources is granted only to authorized individuals and is restricted to only what is required based on job function, need-to-know, employment status, and management approval.*

2.4. *HSF computing and information resources may only be used for HSF business purposes and for no other reason.*

2.5. *All HSF personnel must comply with the following information and data protection areas:*

2.6. Data Protection Areas

THIS SECTION COVERS ANY UNAUTHORIZED COPYING, UNAUTHORIZED DISTRIBUTION, UNAUTHORIZED REPRODUCTION, UNAUTHORIZED TALKING, AND/OR ABUSE OF DATA OR DOCUMENTS, WHICH ANY OF THEM OR ALL OF THEM MEANS UNCONDITIONAL TERMINATION OF THE EMPLOYMENT CONTRACT.

2.6.1. Kullanici Kimligi ve Sifre: Bilgi ve bilgi islem kaynaklari icin kullanici kimligi ve parola,
2.6.1.1. Kullanici kimligi HSF yonetimi tarafindan atanir,
2.6.1.2. Kullanici sifresi **tamamiyle ve kosulsuz** kullanici sorumlulugundadir,
2.6.1.3. Kullanici sifresi en az 9 karakter icermelidir,
2.6.1.4. Kullanici sifresi buyuk harf, kucuk harf, en az 1 rakam ve en az bir ozel isaret icermelidir,
2.6.1.5. Kullanici sifresi 180 gunde bir degistirilmelidir,
2.6.1.6. Kullanici sifresinin baskasi tarafindan bilincli veya dolayli olarak kullanilmasina destek olmak kosulsuz is akdi feshi anlamina gelir,
2.6.1.7. Kullanici sifresinin baskasi tarafindan kullanilmasindan kaynakli her turlu sorumluluk kullaniciya aitdir.
2.6.2. Mulkiyet: Musteri mulkiyeti altindaki hersey,
2.6.2.1. Her turlu bilgi,
2.6.2.2. Her turlu belge,
2.6.2.3. Her turlu yardimci ekipman,
2.6.2.4. Her turlu diger ekipmanlar,
2.6.3. HSF Mulkiyeti:
2.6.3.1. Kalite yonetim sisteminde tanimli surecleri icin gecerli her turlu belge, dokuman ve ekipman,
2.6.3.2. ERP sistemlerinde kayitli herturlu bilgi, belge ve surec isleyis disiplinleri,

2.6.1. User ID and Password: *The User ID and password for information and computing resources,*
2.6.1.1. *The user ID is assigned by the HSF administration,*
2.6.1.2. *The user password is the **sole and unconditional** responsibility of the user,*
2.6.1.3. *The user password must contain at least 9 characters,*
2.6.1.4. *The user password must contain uppercase and lowercase, at least 1 number, and 1 special symbol.*
2.6.1.5. *The user password must be changed every 180 days.*
2.6.1.6. *Intentionally or indirectly supporting the use of the user password by another person constitutes unconditional termination of employment.*
2.6.1.7. *The user is responsible for any liability arising from the use of the user's password by another person.*
2.6.2. Property: *Everything under customer ownership,*
2.6.2.1. *All kinds of information,*
2.6.2.2. *All kinds of documents,*
2.6.2.3. *All kinds of auxiliary equipment,*
2.6.2.4. *All kinds of other equipment,*
2.6.3. HSF Ownership:
2.6.3.1. *All documents, papers, and equipment applicable to the processes defined in the quality management system,*
2.6.3.2. *All kinds of information, documents and process operating disciplines recorded in ERP systems,*

3. DIGER KONULAR

3.1. Digital Kopya: Genellikle bir bilgisayarda veya baska bir dijital cihazda saklanan bilginin dijital versiyonudur.
3.2. Basili Kopya: Bilginin fiziki cikdi gibi baskili versiyonu veya dokumante edilmis halidir.
3.3. Siniflandirilmamis – Harici Yazismalar: Guvenlik kisitlamasi olmayan, HSF KYS kapsaminda guvenli (kisitlanmis) bilgi bulundurmayan ve ITAR veya Ihracat Lisansi kapsaminda bilgi barindirmayan harici yazismalardir.
3.4. Hassas Bilgilerin Saklanmasi veya Imhasi: Basili kopya halinde veya tasinabilir elektronik ortamda bulunan hassas bilgiler, kilitli bir masada, ofisde veya dolapda ya da kutuda saklanmalidir. Basili kopya halinde bulunan hassas bilgiler, hassas bilgilerin imhasi icin ayrilmis guvenli bir kutuya konulmali veya parcalama gibi yeniden olusturulmasini engelleyecek sekilde imha edilmelidir.
3.5. Uzakdan Erisim: Uzakdan erisim, en yuksek veri guvenligi risk seviyesidir. HSF icin "Uzaktan Erisim", sirket verilerinin bilerek, isteyerek ve kabul edilebilir bir sekilde diger tum kullanıcilara acik olmasi anlamina gelir. HSF bunyesindeki tum kullanicilara hicbir kosulda uzakdan erisim izni verilmez.
3.6. Virusler ve Kotu Amacli Kodlar: Bilgisayar virusu, izniniz ve/veya bilginiz olmadan bilgisayarinizi veya eristiginiz bilgi ve verileri olumsuz etkilemek uzere tasarlanmis ve yazilmis istenmeyen bir komut dizini, eklenti, bilesen veya programlaridir.
3.7. Virus bulasma riskini en aza indirmek icin HSF, her bilgisayarda guncel bir antivirus yazilimi kullanir.

3. OTHER RULES

3.1. Soft Copy: *It is a digital version of information, usually stored on a computer or other digital device.*
3.2. Hard Copy: *A printed version or documented form of information, such as a physical printout.*
3.3. Unclassified – External Correspondence: *It is external correspondence that has no security restrictions, does not contain confidential (private) information within the scope of HSF QMS, and does not contain information within the scope of ITAR or Export License.*
3.4. Storing or Disposing of Sensitive Information: *Sensitive information in hard copy or on portable electronic media must be secured in a locked desk, office, or cabinet or container. Sensitive information in hard copy form should be placed in a secure container designated for disposal of sensitive information or otherwise destroyed in a manner that precludes its reconstruction, such as shredding.*
3.5. Remote Access: *Remote access is the highest data security risk level. For HSF, "Remote Access" means that the company data is knowingly, voluntarily, and acceptably exposed to all other users. Remote access is not allowed for all users under any circumstances within the HSF company.*
3.6. Viruses and Malicious Codes: *A computer virus is an unwanted script, plug-in, component or program that is designed and written to adversely affect your computer or the information and data you access without your permission and/or knowledge.*
3.7. *To minimize the risk of contracting a virus, HSF requires up-to-date anti-virus software on every machine.*

3.7.1. Ek onlemler sunlardir:

3.7.1.1. Ekleri ve indirilen dosyalari acmadan once kaydetmek ve taramak.

3.7.1.2. Riskli dosya turlerini (.exe, .bat, .vbs, .scr) engellemek veya acmamak.

3.7.1.3. Duzenli olarak tam disk virus taraması calistirmak.

3.7.1.4. HSF haftalik tarama yapılmasini onerir.

3.8. Ag Guvenlik Onlemleri: Ag guvenlik aciklari, HSF surec verilerine erişebildiği kolaylastirabilir ve HSF bilgilerini tehlikeye atabilir. Bu nedenle ag erisimi olan her kullanici sunlari yapmalidir:

3.8.1. Otomatik yanitlama ozelligine sahip masaustu modemleri yasaklayin.

3.8.2. Bilgisayar sistemlerindeki tum gereksiz programlari ve islevleri devre disi birakin.

3.8.3. Parolasi olmayan veya varsayilan parolalari olmayan hesaplari devre disi birakin.

3.8.4. Kullanicilar ayrildiginda veya is sorumluluklarini degistirdiğinde hesaplari derhal silin.

3.8.5. Baskasinin bilgisayarini asla ve hicbir kosulda kullanmayin.

3.9. Lync (Sanal Toplanti) Hizmetleri: Lync Hizmetleri, HSF internet güvenlik duvari araciligiyla gercek zamanli toplantilar ve is birligi oturumlari duzenleyerek, dahili HSF kullanicilari ile HSF disindaki is ortaklari, musteriler ve tedarikciler arasinda sanal veri alisverisini kolaylastirir. Bu nedenle, Lync Hizmetleri kullanilarak paylasilan tum bilgiler hassas bilgi koruma yonergelerine ve HSF'nin gerekliliklerine uygun olmalidir.

3.10. Lync Hizmetleri Kullanicilarini Dogru Sekilde Tanımlayin: Sanal toplantinin uyumlu olmasini saglamak icin, toplanti katilimcilari ve ilgili erisim duzeyleri dogru bir sekilde tanimlanmali ve paylasilan tum bilgiler dogru sekilde etiketlenmelidir.

3.11. Bir Lync Hizmetleri oturumu duzenlerken, tum toplanti katilimcilari tanimlamak ve tanimak toplanti sahibinin sorumlulugundadir.

3.12. Lync Hizmetleri, hassas, ozel veya disa aktarimi kontrollu verilerin paylasilacagi bir toplantiya kimlik dogrulama olanagi saglar. Boyle bir toplantiya kimlik dogrulamasi yapmak icn bir hesaba ihtiyaciniz olacakdir.

3.13. Toplanti sahibi, kimligi doğrulanmamis konuklarin erisimini reddedebilir. Hassas bilgi paylasilmiyorsa, toplantiya kimligi dogrulanmamis bir konuk olarak kabul edilebilirsiniz.

3.14. Bir Uygulamanin Kontrolunu Paylasirken Dikkatli Olun: Sanal toplantilar, PowerPoint, Word ve Excel gibi uygulamalarin ekranlarinin paylasilmasiyla ilgilidir. Ekran paylasimina ek olarak, toplanti yazilimi paylasilan bir uygulamanin kontrolunu baska bir toplanti katilimcisina vermenize de olanak tanir. Bir uygulamanin kontrolunu paylasirken lutfen dikkatli olun. Bir uygulamanin kontrolonu verdiğinizde, uzak kullanicinin etkinliklerini her zaman izleyin. "Dosya Ac" komutu gibi onaylanmamis etkinlikler fark ederseniz, uzaktan kontrol ayricaligini kaldırmak icin hemen "ESC" tusuna basin. Bir uygulamanin uzakdan

3.7.1. *Additional measures include:*

3.7.1.1. *Saving and scanning attachments and downloaded files before opening them.*

3.7.1.2. *Blocking or not opening risky file types (.exe, .bat, .vbs, .scr).*

3.7.1.3. *Running full disk virus scan on a regular basis.*

3.7.1.4. *HSF recommends weekly scanning.*

3.8. Network Security Measures: *Network vulnerabilities can facilitate access to HSF process data and compromise HSF information. Therefore, any user with network access should:*

3.8.1. *Ban desktop modems which have auto-answer features.*

3.8.2. *Disable all unnecessary programs and functions on computer systems.*

3.8.3. *Disable accounts that have no password or default passwords.*

3.8.4. *Immediately delete accounts when users leave or change job responsibilities.*

3.8.5. *Never, under any circumstances, use someone else's computer.*

3.9. Lync (Online Meeting) Services: *Lync Services conducts real-time meetings and collaboration sessions through the HSF Internet firewall, facilitating virtual data exchange between internal HSF users as well as partners, customers, and suppliers outside of HSF. Therefore, any information shared using Lync Services must follow the sensitive information protection guidelines and HSF proprietary requirements.*

3.10. Properly Identify Lync Services Users: *To ensure the virtual meeting compliance, meeting participants and their corresponding access levels must be accurately identified, and any shared information must be properly labeled.*

3.11. *When hosting a Lync Services session, it is the host's responsibility to identify and recognize all meeting participants.*

3.12. *Lync Services provides the ability to authenticate to a meeting in which sensitive, proprietary or exportcontrolled data will be exchanged. To authenticate to such a meeting, you will need an account.*

3.13. *A meeting host may deny access to unauthenticated guests. If no sensitive information is being exchanged, you may be admitted to the meeting as an unauthenticated guest.*

3.14. Use Caution When Sharing Control of an Application: *Virtual meetings are all about sharing displays of applications such as PowerPoint, Word, and Excel. In addition to sharing displays, the meeting software also allows one to give control of a shared application to another meeting participant. Please use caution when sharing control of an application. If you give control of an application, always monitor the remote user's activities. If you notice unapproved activities such as use of the "File Open" command - immediately hit the "ESC" key to take away the remote-control privilege. Handing off remote*

kontrolunu devretmek, kisinin kimliginizi ustlenmesine ve ibilgisayarinizin ve bagli tum ag kaynaklarinin tam kontrolunu ele gecirmesine olanak taniyabilir. Uygulamanin gozetimsiz kontrolune izin verilirse, dosyalar silinebilir, kotu amacli web siteleri ziyaret edilebilir ve bilgisayarinizdan hassas dosyalar alinabilir.

control of an application may give the person the ability to assume your identity and take complete control of your computer and all attached network resources. If unsupervised control of the application is permitted, files could be deleted, malicious web sites could be visited, and sensitive files could be retrieved from your computer.