



MCOR-IT-520 User Information Security Policy

Document Owner: Pilar Simón – CTO	Verified: Albert Clarà – CISO	Approved: Francesc Chavarria – CIO Pascal Guichard – CEO
21/2/22	21/2/22	21/2/22

Copyright © Merit Automotive Electronics Systems. This document, and the information it contains, is the intellectual property of Merit. No part of this document may be reproduced, altered, stored in a retrieval system, or transmitted in any form, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Merit.

Contents

1. INTRODUCTION	3
2. SUMMARY FOR ALL STAKEHOLDERS	4
3. GENERAL TOPICS	6
3.1. End User Responsibilities	6
3.1.1. Blog/Internet Posting	6
3.1.2. Chat/Instant Messaging (IM)	7
3.1.3. Email	8
3.1.4. Hardware Assets	8
3.2. Information Protection	9
3.2.1. Classification	9
3.2.1.1. Public	10
3.2.1.2. Internal Use	10
3.2.1.3. Confidential	10
3.2.1.4. Restricted	11
3.2.2. Disclosure	11
3.2.3. Disposal	12
3.2.4. Hardcopy Controls	12
3.2.5. Labelling	12
3.2.6. Retention	13
3.3. Internet Security	13
3.3.1. Cybersecurity	13
3.3.2. Downloads and Executable Files	13
3.3.3. Hacking	14
3.3.4. Identity Theft	14
3.4. System & Application Access	15
3.4.1. Accountability	15
3.4.2. Authentication	15
3.4.3. Authorization	15
3.4.4. Authorized/Approved Devices	16
4. DISCLAIMER	17
5. GLOSSARY	18
6. REVISION RECORD	20
7. ACCEPTANCE	21

1. Introduction

Information Security Policy

MERIT's information and IT systems must be adequately safeguarded to enable the company to efficiently, effectively, and safely conduct operations. To that end, a control environment based on the ISO 27001 standard will be established and maintained to effectively recognize and mitigate Information Technology-related risks which impact the business.

To ensure that an adequate information security control environment within MERIT is established and maintained, the CIO will be responsible for management of the information security policy and coordination of all actions related to its instructions, including any required engagements with external parties.

The MERIT Information Security Council (MISC), comprised of representatives from the different units and security support organizations, provides management direction and high-level steering of security direction and programs.

MERIT's Information Security Council is responsible for the following actions:

- *Review and approve information security policies*
- *Assign information security roles and responsibilities*
- *Monitor for significant changes and exposure of company information assets to security threats.*
- *Review and monitor security related incidents*
- *Review and approve initiatives aimed at improving information security*

2. Summary for all stakeholders

MERIT computing and data communications are valuable and limited resources that serve a large number and variety of users. (NOTE: A “user” is any MERIT person, including permanent/full- time employees, temporary employees, like so, contractors, and any other individual that is working with or on behalf of MERIT, and/or has access to MERIT information or resources.)

These policies apply to all users of MERIT information globally, including visitors, contractors, suppliers and employees.

All users have the responsibility to make use of these resources in an efficient, ethical, and legal manner.

These policies also apply to all information systems owned, contracted, leased or operated for or by MERIT, connected to the MERIT network, or used to process, stored or transfer MERIT data.

MERIT reserves the right to scan and monitor system access and use according to each country applicable legislation.

Merit’s computer and network services provide access to resources both within and outside the MERIT environment.

These services must be used in a manner consistent with the mission and objectives of MERIT and with the purpose for which such use was intended.

Access to MERIT’s data and resources is a privilege and imposes upon user’s certain responsibilities and obligations, and is subject to MERIT policies, and applicable laws.

Acceptable use is always ethical, reflects professional integrity, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, protection of sensitive information, ownership of data, copyright laws, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

All activities inconsistent with these objectives are considered to be inappropriate and may jeopardize continued use of computing facilities and networks.

In consideration of being allowed to use the MERIT computer, network, and other IT services, all users must understand and agree to the following:

1. Users shall not use the Resources for any illegal activity or for any activity prohibited by this policy (see subsequent examples of inappropriate conduct that is prohibited).
2. Users agree not to use the Resources to infringe upon or otherwise impair, interfere with or violate any copyright or other intellectual property rights of another. This pertains to all MERIT intellectual property as well as copyrighted material, including, but not limited to music, video and software.
3. Users shall avoid any action that interferes with the efficient operation of the Resources or impedes the flow of information necessary for conduct of MERIT business.
4. Users shall protect their computer resources such as ID, logins and systems from unauthorized use. Users are responsible for reasonably securing their computer, including implementing such protections as logins to prohibit unauthorized use.
5. Users will access only information that is their own, or to which their access has been authorized. Users will only access networks, network resources, and information for their intended use.

6. User shall immediately report any known or suspected violations of this policy to the informationsecurity@merit-automotive.com mailbox.

Examples of Inappropriate Use of Resources include, but are not limited to:

- Unauthorized access to another person's computer, computer account, files, or data.
- Using the MERIT network to gain unauthorized access to any computer system.
- Using any means to decode or otherwise obtain restricted passwords or access control
- Attempting to circumvent or subvert system or network security measures. Examples include creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system.
- Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to MERIT data.
- Performing any act, intentionally or otherwise, that will interfere with the normal operation of computers, peripherals, or networks.
- Making or using illegal copies of copyrighted software, storing such copies on MERIT systems, or transmitting them over MERIT networks.
- Harassing or intimidating others via electronic mail, news groups or Web pages.
- Initiating or propagating electronic chain letters.
- Initiating or facilitating in any way mass unsolicited and unofficial electronic mailing (e.g., spamming, flooding, or bombing).
- Forging the identity of a user or machine in an electronic communication.
- Saturating network or computer resources to the exclusion of another's use, for example, overloading the network with traffic such as emails, excessive file backup/archive, or malicious (denial of service attack) activities.
- Using MERIT systems or networks for personal gain; for example, by selling access to your ID or to MERIT systems or networks, or by performing work for profit with MERIT resources in a manner not authorized.
- Engaging in any other activity that does not comply with the general principles presented above.

3. General Topics

3.1. End User Responsibilities

3.1.1. Blog/Internet Posting

With the proliferation of social media and next generation communication tools, the means by which MERIT employees can communicate internally and externally continue to evolve.

Although these tools provide exciting and new opportunities for communication and collaboration, they also create new responsibilities for MERIT users.

These social media posting guidelines apply to users who use the following to post MERIT-related material either from home or work:

- Multi-media and social networking websites including, but not limited to: LinkedIn, Facebook, Instagram, Twitter and YouTube
- Blogs
- Wikis such as Wikipedia and any other site where text can be posted.

Social media involvement is a personal choice for each user.

If you choose to utilize any of the various social media sites available, you should exercise caution and discretion when deciding whether to post information that may relate to MERIT.

Common sense is your best guide. If you are unsure about any particular posting, please contact a member of the MERIT HR Department for guidance.

If you are participating in social media or decide to participate, you must follow the guidelines provided below.

A violation of these guidelines by posting MERIT material in an inappropriate manner may result in disciplinary action up to and including termination of employment.

1. Human Resource Policies

- Understand and adhere to the employee conduct standards outlined in MERIT's Human Resource Policies and the MERIT Code of Business Conduct when involved with social media.
- Do not use slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in MERIT's workplace.

2. Confidential Information

- Do not disclose any information that is confidential or proprietary to MERIT or to any third party that has disclosed information to MERIT.
- Do not comment on confidential MERIT financial information such as MERIT's future business performance, business plans, or prospects anywhere in world or any financial information about a current or prospective customer, supplier or partner of MERIT. This includes statements about an upcoming quarter or future performance data or information about alliances, and applies to anyone including conversations with analysts, journalists or other third parties.

3. Transparency

- When discussing MERIT or MERIT-related matters, you must clearly identify yourself as a MERIT employee or affiliate in your postings or blog site(s) and include a disclaimer that the views are your own and not those of MERIT.
- An example of an appropriate disclaimer is "The postings on this site are my own and don't necessarily represent MERIT's positions, strategies, or opinions."
- Be aware of your association with MERIT in online social networks. If you identify yourself as a MERIT employee or collaborator, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and business relations.

4. Legal Matters

- Do not comment on anything related to legal matters, litigation, or any parties with whom we are in litigation.
- You are legally responsible for your postings. If your posts are found to be defamatory, harassing, or in violation of any other applicable law(s), you may be subject to civil and/or criminal liability.

3.1.2. Chat/Instant Messaging (IM)

All IM communications and information transmitted, received, or stored in the MERIT internal IM system belong to MERIT. Users have no reasonable expectation of privacy when using IM. MERIT reserves the right to monitor, access, and disclose all employee IM communications.

Always use professional and appropriate language in all instant messages. Users are prohibited from sending abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive instant messages.

3.1.3. Email

MERIT does not read users' emails as a matter of course, but in cases of suspected misuse, the company reserves the right to examine email messages without authorization from or notification to the sender or recipient to the extent permitted by applicable privacy laws.

No individual monitoring of users will take place without authorization required by applicable law. All guidelines and policies supporting applicable law will be followed after internal approval from HR has been obtained.

Users must not use profanity, obscenities or derogatory remarks in any email messages discussing employees, customers, competitors or others involved with MERIT business. Sexual, racial, or other forms of harassment are strictly prohibited.

Email accounts, like user IDs, are for specific individuals and must not be shared. Approved group mailboxes are allowed.

After termination of employment, the user's account must be disabled. Access to a former user's existing mail file must be approved by I.T. and HR.

If a user is unable to check their mail for extended periods, access to the Inbox can be granted to another MERIT user. If a user will be out of the office for a short period of time, the out of office notification tool should be enabled.

No systematic forwarding of electronic communications to addresses outside of MERIT is permitted. Likewise, outside email addresses are not to be used to conduct MERIT business at any time.

If an email contains sensitive information, users must not forward it to another recipient unless the other recipient is known to be authorized to view the information or the originator approves the forwarding. Forwarding of a former user's inbound email to their replacement and/or manager does not require approval.

Broadcast message distribution must not be utilized unless department manager approval has been obtained. Selected distribution lists will be used wherever possible, and do not require approval.

3.1.4. Hardware Assets

Users are responsible for safeguarding any MERIT hardware in their possession. Laptops, tablets, smart phones and other mobile IT devices must be kept physically secure at all times. If left overnight, these devices must be locked in a drawer or cabinet. Avoid leaving hardware in vehicles, particularly in plain sight. Promptly report any lost or stolen hardware to the Service Desk, local police, and local security staff.

Managers are responsible for collecting the hardware from users who stop providing services or collaborating with the company. IT must be notified before re-issuing any hardware.

Acceptable Use of Computing Resources

Users are responsible for exercising good judgment regarding appropriate use of MERIT resources in accordance with MERIT policies, standards, and guidelines. MERIT resources may not be used for any unlawful or prohibited purpose.

Incidental personal use of MERIT information systems, including the telephone, is permissible as long as the usage does not:

- Interfere with job performance (ex. incessant instant messaging)
- Deny other users access to system resources (ex. streaming video)
- Incur significant costs (ex. international phone calls)

Use of software licensed to MERIT on a personal computer (not owned by MERIT) is not authorized unless the system has been designated a system that is used to process MERIT information.

Users must not test or attempt to compromise any information security mechanism unless specifically authorized to do so by Information Security. Users must not possess software or other tools that are designed to compromise information security.

Installation of personal or non-IT approved software is prohibited.

3.2. Information Protection

Information protection involves providing the necessary control structure to avoid inadvertent or intentional disclosure or compromise of MERIT data, whether in electronic, hardcopy, or another format. In order to protect information, it must be appropriately identified (particularly with respect to location/sources of data), classified, restricted (access-controlled), and owned.

MERIT information is a corporate asset, and is authorized for use on only those devices, systems, applications, and processing techniques that are approved by MERIT; it is not authorized for personal use, for use on unauthorized devices, systems, applications and processing techniques, and must never be forwarded to a personal account.

3.2.1. Classification

There are four information classification designations: public, internal use, confidential, private; each of which defines how data is to be adequately secured. The data types listed below are described in order of least to most restrictive, in terms of access and associated security and protective controls.

3.2.1.1. Public

Information of this type would include press releases, published financial information and product/content information that is disclosed on www.merit-automotive.com.

Corporate Communications, and the Corporate Controller are typically the only groups authorized to release public information.

Users are not permitted to classify and release any information to the public, without prior approval from a designated authority at MERIT.

Most information at MERIT is not public data, and is not subject to disclosure. There are no specific protection requirements associated with public information.

3.2.1.2. Internal Use

Internal use information would include specifics on MERIT operations and operating procedures, project-related details (including budget, schedule, and overall status), group meeting subjects and internal policies and procedures (such as this document) that are covered by a contract, and the contract agrees on sharing Merit's information with the customer.

Contract must state what happens with information when the contract ends, like returning or destroying it.

Unless otherwise designated, all information at MERIT is considered at least Internal Use, and should not be discussed, disclosed, or otherwise distributed to non-MERIT or non-authorized personnel [personnel is authorized when a NDA or similar exist between this particular and Merit].

All users must exercise due care to prevent the public release of this information.

Only designated information owners at MERIT are permitted to disclose this information, or otherwise classify with a different designation.

There will typically be no restrictions on the movement or release of this information within MERIT.

However, permissions-based or role-based access controls may be implemented to protect electronic data as deemed necessary by the information owners.

Additional protection in the form of encryption or segmentation is usually not warranted.

Internal Use information will be protected from external threats through the use of network perimeter defences (such as firewalls).

3.2.1.3. Confidential

Information of this type includes engineering data, intellectual or industrial property, merger and acquisition details, pre-public release financial information, pricing and margin data, and specifics surrounding customer, vendor, or supplier relationships.

Confidential information is not for open disclosure among all MERIT users; by its nature, it is to be disclosed only on a need-to-know basis and at the discretion of the primary data owner.

In addition to the protection and controls noted for Internal Use, other measures such as restricted folders, protected network drives, segmentation, and encryption methods will be employed.

Confidential information should not be stored, managed, or released on common-access network devices or non-secure areas, to include: shared drives, public-access printers, or in physical environments that do not afford some level of reasonable protection and security. Confidential information may not be reproduced or copied without proper authority or approval.

3.2.1.4. Restricted

Restricted information includes any data that could result in the identification of sensitive and personal (individual) information about a user, customer, or supplier/vendor that is otherwise not publicly available. There is increased public sensitivity around Restricted information due to the risk associated with disclosure or breach of this information. Risks to MERIT include, reputation, financial, and legal/litigation exposure, which are highlighted in numerous laws and other regulations intended to protect personal/private data.

Examples of private information include social security number, bank routing or other financial information, passport number, credit card number, or other information that is linked or linkable to a specific individual.

Private information is the most restricted data at MERIT, with only few users having a reason to have access to, or otherwise possess this information. In most cases, only Human Resources (HR) users have a need to regularly maintain or use this information during the performance of employment agreements with MERIT employees. Customer, supplier/vendor information (that relates to specific individuals) may also have a need for specific oversight and regulation and will be the responsibility of the appropriate organizations.

The same protection and controls noted for Confidential information will apply to Private data, with an emphasis on highly restricted access, and segmentation from other MERIT information. The reproduction or copying of Private information may not be done without proper authority or approval and when permitted by applicable laws.

3.2.2. Disclosure

Only Public information is available for disclosure outside of MERIT. Internal Use information is generally not permitted for outside disclosure, and Confidential and Private information is further restricted, and is only available to authorized data owners.

Only authorized data owners have the authority to release Confidential and Private MERIT information, whether to internal users or external stakeholders, when permitted by applicable laws.

When non-public information is disseminated outside of the MERIT domain by the appropriate users, a Non-Disclosure Agreement (NDA) must be signed and kept on file to protect MERIT information from further disclosure to third parties.

3.2.3. Disposal

When corporate information is deemed no longer useful or necessary, it must be properly disposed of to prevent inadvertent or accidental disclosure.

For hardcopy information, MERIT facilities provide the means to securely dispose of corporate information. These include shred bins and shredders. Hardcopy information classified as Internal Use, Confidential, or Private should never be disposed of in receptacles designated for ordinary waste (e.g. trash can).

Electronic medium, to include CDs/DVDs, flash drives, flash memory, hard drives, legacy computer or computing devices, secure digital (SD) or other micro cards, etc., should be provided to the local IT support team for proper disposition and disposal.

The I.T. Team will be responsible for providing specific instructions and criteria for proper disposal of electronic media, and must oversee, approve, and record the disposal methods and processes for all computer, network, and other IT related storage devices.

3.2.4. Hardcopy Controls

Corporate information in hardcopy format can be easily manipulated and modified.

The original content, message, or intent of the document can be subject to inadvertent or intentional modification.

All documents of record, to include policies, procedures, standards, etc., and contractual documents with external parties, should be saved in a format that prevents the original document from being altered.

The preferred means to protect these documents is to save them in a Portable Document Format (.pdf extension), such as Adobe Acrobat, where future modification can be controlled.

3.2.5. Labelling

All MERIT information should be properly labelled. For hardcopy information, the header of each page of each document should be labelled with the appropriate classification, as follows:

Internal Use – Not for disclosure without a signed NDA or similar.

Confidential – MERIT information. Do not disclose.

Restricted– Highly sensitive and restricted MERIT information. Access is need-to-known only.

Electronic medium (examples noted above) should be labeled along the same guidelines, to the extent possible and practical.

3.2.6. Retention

Data retention requirements are defined according to the appropriate, specific business requirements. Consult the relevant record retention schedules.

3.3. Internet Security

Any device on the internet has the ability to share information with any other device that is also on the network (the internet).

With this connectivity comes great opportunity and access to data, along with substantial risk of compromise of information, infection of malicious code or software (collectively called malware), or inadvertent access to information that is otherwise not of interest, or worse, considered offensive or harmful.

All users should become familiar with the content relating to internet security in an effort to protect them, as well as IT resources,

3.3.1. Cybersecurity

Cybersecurity is defined as the processes, tools, and procedures employed to effectively mitigate the threats posed by using or connecting to the internet.

These include blocking sites that are known to promote malicious software, employing the use of endpoint protection software (such as anti-virus), and user awareness and training.

All users are responsible for ensuring these security measures are understood and are not purposefully circumvented.

3.3.2. Downloads and Executable Files

Users are encouraged to download only that content that is relevant to the execution of their activity, provided the site is considered trusted (known to be a legitimate web presence), and is not otherwise blocked by the I.T. Team.

Applications and programs are specifically not authorized for download, unless provided for by the Service Desk.

This applies in particular to any peer-to-peer file or information sharing programs.

Any executable files are also prohibited, as these are known methods for distribution of malware.

Examples of executable files include (as an example) the following extensions: *.bin, *.cgi, *.cmd, *.dll, *.exe, *.ex4, *.inf, *.ins, *.sys, *.msi, *.bat.

Never download, open, or execute any attachment in an email unless the originator (sender) is trusted, and the content is clear and relevant.

Hackers will often use hijacked email accounts for a compromised user's legitimate address book to spread malware through attachments to the contacts.

3.3.3. Hacking

Hacking is intentional attempt to gain unauthorized access, to computer systems, files, or information. While sometimes innocent in nature, hacking is often malicious in intent, with the objective of bypassing any security or controls to gain illicit access.

Hackers are often associated with criminal activity and organized crime, and will use techniques such as phishing or social engineering (described below) to obtain desired information.

Hacking is a prohibited activity for all MERIT users. Anyone that suspects another user of hacking should contact the MERIT ETHICS HOTLINE: linea.etica.merit@merit-automotive.com.


3.3.4. Identity Theft

One of the greatest risks of internet usage is the theft of an individual's identity.

This can occur when personally identifiable information is obtained without permission in order to conduct fraudulent activity, typically involving financial misrepresentation or outright monetary theft.

All users should be aware of this risk, and should be vigilant with their personal data.

The following guidelines should be understood and adhered to:

- Provide financial data or personally identifiable information only when dealing with a trusted site or organization.
- Provide financial data or personally identifiable information in an online/internet transaction only when the Uniform Resource Locator (URL) or website address commences with an "https" ("s" indicates transaction level security is enabled), or displays a lock icon  indicating a secure connection.
- Provide only information that you are comfortable with, and that seems sensible. There should be limited instances when a social security number or specific bank information (such as routing number, account number, etc.) are actually required.
- Shred or otherwise securely dispose of any information that contains personally identifiable information or sensitive financial information. Do not throw directly into the trash without removing this information.
- Regularly review your credit reports, as well as financial statements (credit card statement, bank account statement) etc., to determine if fraudulent or suspicious activity is present.

3.4. System & Application Access

Access to MERIT systems and information is enabled through the user identification (user ID).

A user ID, with an associated password, is an asset.

If compromised, it can result in the inadvertent disclosure of information, which can create financial, legal, and reputation risk. All users have a primary responsibility to protect their individually assigned user ID(s) to ensure unauthorized use is not enabled.

The following guidelines must be understood and adhered to with respect to system access.

3.4.1. Accountability

Individual user accounts (user ID) shall be created for all users to ensure accountability for all system/application usage.

Each user ID and password is intended for the exclusive use of the designated user.

Users are responsible for all activity that occurs with their designated user ID.

Do not share the user ID with anyone, except Information Technology (IT) support personnel, and then only for troubleshooting and resolving issues. After troubleshooting and support is completed, change the password immediately.

Do not share your password with anyone. **The MERIT service desk will never ask for your user ID and password to help resolve or trouble shoot an issue.**

Notify the I.T. Team at helpdesk@merit-automotive.com if there is suspicion that a user ID or password has been compromised.

Immediately change any password that may have been disclosed. Users should contact the IT Service Desk to remove any access to application(s) or system(s) that is/are no longer required, and when leaving/returning from an extended leave of absence.

3.4.2. Authentication

Authentication is a means to determine whether an individual or thing is who or what is stated.

Authentication is most often accomplished through the use of a user ID and password.

All MERIT users are required to authenticate prior to accessing the network, or systems/applications.

3.4.3. Authorization

Authorization is the process of providing system-related permission(s).

In the case of Information Systems, this implies access to the data and information is granted through an assigned role within the system. MERIT employs role-based access control(s) to ensure users have rights to information based upon a need-to-know basis, which not only protects information but also helps to avoid Segregation Of Duties (SOD) violations.

An SOD violation potentially allows a user more rights than necessary to perform a given role, and can result in financial and operational risks, including fraud and financial statement reporting concerns.

SOD conflicts are generally not permitted and should be avoided wherever possible.

If an SOD conflict does exist, the appropriate MERIT authority (such as a user working in a controller position) should agree with the exception (including a sign-off) and ensure appropriate mitigating controls are in-place and reviewed regularly.

3.4.4. Authorized/Approved Devices

Only authorized/approved devices and software are permitted in the MERIT environment.

4. DISCLAIMER

Any non-compliance of this policy with local legislation will only invalidate the applicability of the referred point, remaining the rest of the object of the policy. For the legal jurisdiction, Barcelona, Spain is taken as the legal place.

5. Glossary

- **Anti-malware:** is a type of software program designed to prevent, detect and remove malicious software (malware) on IT systems, as well as individual computing devices.
- **Anti-spam:** refers to any software, hardware or process that is used to combat the proliferation of spam or to keep spam from entering a system.
- **CPU:** The central processing unit (CPU) is the unit which performs most of the processing inside a computer.
- **Cryptography:** is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication.
- **DLP (Data Lost Prevention):** refers to the identification and monitoring of sensitive data to ensure that it's only accessed by authorized users and that there are safeguards against data leaks.
- **DMZ (Demilitarized zone):** is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN).
- **E-Business:** business done through the Internet.
- **Firewall:** is software used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet.
- **FTP (File Transfer Protocol):** It is a way to share files over the net.
- **HTTP (Hypertext Transfer Protocol):** is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access.
- **ID:** short form for identification
- **IM:** instant messaging
- **IP:** Internet Protocol
- **IP SEC:** Internet Protocol security
- **ISO 27001:** is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

- **ISO 9000:** is a series of standards, developed and published by the International Organization for Standardization (ISO), that define, establish, and maintain an effective quality assurance system for manufacturing and service industries.
- **TISAX:** is a set of requirements to protect industrial property according with VDA best practices.
- **IT:** Information Technology.
- **LAN:** Local Area Network.
- **NDA (Non-Disclosure Agreement):** is a legal contract between two or more parties that signifies a confidential relationship exists between them.
- **POC (Proof of Concept):** is a demonstration, the purpose of which is to verify that certain concepts or theories have the potential for real-world application. POC is therefore a prototype that is designed to determine feasibility but does not represent deliverables.
- **RAT:** Remote Administration Tool.
- **SSH (Secure Shell):** is a cryptographic network protocol for operating network services securely over an unsecured network.
- **WLAN:** Wireless Local Area Network.

6. Revision Record

Version	Change Description	Date
01	Creation Document	12/12/2018
02	Review	20/12/2019
03	Added acceptance and signature end page. Visual change.	15/09/2020
04	Annual Review	08/03/2021
05	Annual Review	18/1/2022
06	Internal review	21/2/2022

7. Acceptance

In (location) _____ Date : ____ of _____ 20__

MERIT is a company whose purpose is the excellence of the services it provides. MERIT is committed to complying with ISO27001, TISAX and RGPD as a means to provide value to its customers and protect the personal information that is conferred on it in accordance with the best security practices and information protection.

As a MERIT policy user, I acknowledge at this time having received training / awareness in security and protection of personal data, understanding and committing myself to follow and enforce the user security policy "MCOR-IT-520 User Information Security Policy" as well as the MERIT RGPD guidelines.

Name: _____

With ID/DNI/NIE/Passport/ _____ : _____

Signature:
