Acceptable Use Policy for Offsite Development Partners

Document ID: IMS-00161

Revision: 2

Contents

Contents 1
1 Purpose 2
2 Scope 2
2.1 What is confidential data/confidential information? 2
2.2 What is an information Asset? 3
3 Related policies and other documentation 3
4 General Policy concepts 3
5 Detailed Policy concepts 4
5.1 Network 4
5.2 E-mail 5
5.3 Internet 5
5.4 IT Equipment 6
5.3.1 iDirect Provided Computer (Laptop/Desktop) 7
5.3.2 Non iDirect Provided Computer (Laptop/Desktop) 8
5.3.3 Mobile devices (smartphone or tablet) 9
5.3.4 Portable media (USB keys and removable disk drives) 10
6 Information Security Incident Reporting 11
7 Compliance 12
7.1 General deviations 12
7.2 Disciplinary actions 12
8 Revision Management 13
8.1 Document Change Log 13
8.2 Review & Approval Responsibilities 13

1 Purpose

The purpose of this policy is to outline the acceptable use of ST Engineering iDirect ("iDirect") information assets while under engagement with iDirect. This policy is not meant to replace policies already in-place with the contracted person's employer, but to complement them. If there is a component in this policy that conflicts with any component in an existing security policy, the most stringent recommendation will be used.

ST Engineering iDirect's portfolio of products includes items and services that are subject to various multinational laws, rules, and regulations. These rules may dictate where specific products can be taken, sold, or used, and what information about these products can be shared and with whom. Illegal/Inappropriate use of information assets exposes ST Engineering iDirect to information security risks. This policy is in place to protect the confidential data of ST Engineering iDirect, its employees and its business partners from intentional or unintentional information leakage, alteration or destruction caused by the misuse or abuse of ST Engineering iDirect information assets when working on premise, from home or when travelling.

2 Scope

The scope of this Acceptable Use Policy applies to external development partners, off-site contractors, and consultants who do not work from an iDirect office location but require remote access to iDirect systems to perform their work.

This policy governs the use of all information (including hard copies), electronic and computing devices, and network resources for conducting iDirect business or accessing internal networks and business systems, regardless of whether these resources are owned or leased by iDirect, the employee, or a third party.

General deviations (exceptions) to this policy, and disciplinary actions relating to this policy can be found within the compliance section.

2.1 What is confidential data/confidential information?

The term Confidential Information means and includes, without limitation, all currently existing and hereafter created non-public information, whether written or oral, and whether in the form of documentation; correspondence; employee, operating, or other manuals; memoranda; reports; records; notes; computer-retained information; or otherwise, including, without limitation, materials information, processes, procedures, methods, techniques, formulae, know-how, configurations, products, services, advertising or promotion, research, inventions, improvements, innovations, insignias, logos, customers, suppliers, employees, licensees, patents, copyrights, trademarks, trade names, trade secrets, service marks, pricing policies, financial information, intellectual property rights, or other information owned by or relating to the Protected Party, or acquired by the Protected Party under terms limiting or protecting disclosure, that has been identified or labelled as

"Confidential" or is of a nature that the Protected Party would reasonably anticipate the Recipient would treat as confidential.

1. *2.2 What is an information asset?*

An information asset can be described as information or data that is of value to the organization, including such information as patent records, intellectual property, or customer/employee information. These assets can exist in physical form (on paper, CDs, or other media) or electronically (stored on databases, in files, on personal computers).

3 Related policies and other documentation

All iDirect policies and procedures can be found in the Company's Document Management System. These policies will be provided to you by your iDirect contact as required.

4 General Policy concepts

- ✓ Do not share your iDirect credentials with anyone.
- ✓ You must complete all assigned training at your earliest opportunity to maintain your access to the iDirect network.
- ✓ Do not share iDirect Confidential Information to non-iDirect employees or contractors and do not hold confidential conversations in a public place, venue or forum.
- ✓ Do not travel with iDirect confidential data, except per Section 5.4.1 below.
- ✓ You must work in an area that minimizes disruption and where you can maintain confidentiality.
- ✓ You are not allowed to work from Cuba, Iran, North Korea, Syria, China, Hong Kong, Russia, Venezuela, Belarus or any country on the U.S. embargo list.
- ✓ Only software that has been security reviewed and approved can be installed on iDirect systems.
- ✓ All requests for additional permissions, system access, software, VPN updates must be requested via the Service Desk ticketing system.
- ✓ You are only allowed to connect to the iDirect network utilizing the iDirect VPN. No other remote access methods are allowed. Any detection or use of unapproved remote access methods will result in disciplinary action.

- ✓ iDirect requires that you encrypt your computer's hard drive to the AES 256-bit cipher standard.
- ✓ All work output must be regularly updated on the relevant iDirect information platform relevant to the content and as instructed by the iDirect contact for your engagement. Avoid storing any iDirect information solely on your computer.
- ✓ Do not print out any iDirect data unless instructed to do so by your iDirect POC for your engagement.
- ✓ Destroy all iDirect data securely. Hard documents, must be shredded or burnt in a safe manner and disposed of appropriately. Electronic documents must be deleted and if possible the storage device formatted or destroyed.
- ✓ Passwords used to encrypt data must be communicated via a separate communications channel. Example; use SMS to share the password of an encrypted file you are sharing by email.
- ✓ iDirect does not allow the usage of USB drives to store non-public iDirect information as part of your engagement.
- ✓ Protect all devices containing iDirect data to prevent data leakage and do not leave devices unattended and unsecured.
  - ✓ Only connect to secure, password-protected wireless networks whose origin you preferably know.
- ✓ Report immediately any observed or potential theft, loss, or unauthorized disclosure of iDirect data or Equipment (refer to section 6 for more information).
- ✓ Lock your computer screen when you leave your desk.

5 Detailed Policy concepts

5.1 Network

Employees and contractors of ST Engineering iDirect should use the corporate network for professional tasks.

The ST Engineering iDirect networks must be kept secure at all times to protect our intellectual property. It is important to adhere to the following principles:

- ✓ All devices connected to the ST Engineering iDirect's corporate network must be authorised by IT and comply with security baselines and prevailing IT procedures.
- ✓ Firewalls shall mask the internal IP addresses for outbound Internet access.

- ✓ Routing controls shall be defined based on the source and destination address checking mechanism. Appropriate controls shall be implemented to restrict internal addresses so that it cannot pass directly from the Internet and vice versa.
- ✓ Internal Internet Protocol (IP) addresses are controlled and regulated by IT.
- ✓ If any network security weakness is discovered or there is suspicion that the network has been compromised this must be reported to itsecurity@idirect.net immediately.
- ✓ The use of personal IT equipment on the ST Engineering iDirect corporate network is forbidden except if explicitly approved by IT in writing.
- ✓ All downloads from the Internet should not use insecure file transfer protocols like http, ftp, telnet, etc. Whenever possible use a secure protocol, like https, scp, sftp, etc.
- ✓ All uploads/file transfers to the internet must use secure protocols, https, sftp, scp, ssh, etc. Insecure file transfer uploads to the Internet shall not be allowed.

5.2 E-mail

Users of the iDirect e-mail system are responsible for e-mail messages sent and its content(s). This content cannot contain any illegal (advertising for drugs, spreading malware, …) or inappropriate (sexually explicit content, bullying, racism…) messages that could cause harm to iDirect, the sender or the receiver.

E-mail is an unsecure means of communication. It is important to adhere to the following principles:

- ✓ Do not send confidential Information externally via e-mail. Rather, store and share the documents using sharing links from iDirect's OneDrive or SharePoint services.
- ✓ Confidential Information must be encrypted when sent outside of iDirect's communication systems (attachments or body e-mail).
- ✓ Forward unwanted and/or unexpected incoming messages (phishing, spam, unknown/dubious senders, dubious attachments) to phishing@idirect.net.
- ✓ You are not allowed or authorized to use the iDirect e-mail account for private usage, or any other usage that does not relate directly to the iDirect engagement.
- ✓ You are not allowed or authorized to send iDirect information to your own private personal mailbox. You are allowed to send engagement related information to users who are directly involved in the execution of an iDirect contract as long as those mailboxes are maintained by your business.
- ✓ You must not setup email forwarding rules that forwards internal emails externally without explicit permission from itsecurity@idirect.net.

- ✓ Verify if email attachments sent to you are legitimate and verify links before using them. If in doubt, report to phishing@idirect.net.

- ✓ You must not register for internet-based services with your iDirect email address unless the services are required in line with your job function, you believe the site to be trustworthy, and you have approval from your iDirect contact.

5.3 Internet

iDirect's internet connections must only be used for tasks explicitly related to the engagement with iDirect.

It is important to adhere to the following principles:

- ✓ Corporate data must only be stored on supplied tools of iDirect (OneDrive for Business, SharePoint, iDirect corporate network drives, BitBucket, Jira, Confluence). You must not store data solely on your computer's hard drive.
- ✓ You should only exchange confidential data using the STEi approved file sharing mechanisms (SharePoint, or OneDrive for Business). Customers can mandate that we use their file sharing platform as required by the customer. Distribution of company information to non-corporate or unapproved customer file sharing solutions is strictly prohibited;
- ✓ You must not publish iDirect data online (discussion boards, personal blogs, social media, and blogs).

- ✓ Use of internet for illegal/inappropriate purposes (including but not limited to sexually explicit content, digital piracy, harassment, bullying, drug purchase...) is strictly prohibited.
- ✓ Only download and install correctly licenced applications on to iDirect's systems – when in doubt, ask IT or your iDirect point of contact.
- ✓ Review unexpected system messages when browsing the internet from an iDirect system and report anything of concern to itsecurity@idirect.net (browser warnings, certificate warnings).

- ✓ Verify URLs (Uniform Resource Locators). When in doubt, contact the itsecurity@idirect.net.

- ✓ The usage of anonymising services (i.e., private VPN (Virtual Private Network), Tor browser), is prohibited while working on or connected to the resources of iDirect.

- ✓ Scanning of the iDirect production network is prohibited (exception for testing product).

- ✓ All downloads from the Internet should not use insecure file transfer protocols like http, ftp, telnet, etc. Whenever possible use a secure protocol, like https, scp, sftp, etc.

- ✓ All uploads/file transfers to the internet must use secure protocols, https, sftp, scp, ssh, etc. Insecure file transfer uploads to the Internet shall not be allowed.

5.4 IT Equipment

IT equipment issued by iDirect must only be used to conduct activities related to your engagement with iDirect. The use of personal or private computers is forbidden, except in those engagements where consultants or contractors have no other option but to utilise their own equipment to conduct business activities. Such exceptions require approval of your iDirect manager.

5.4.1 iDirect Provided Computer (Laptop/Desktop)

Contractors or consultants of iDirect that have been issued an iDirect laptop must not use the laptop for personal usage. You must not share your laptop with family members or friends, or anyone that is not explicitly authorized under your engagement with iDirect.

Adhere to the following principles, and contact IT in case of a problem:

Receiving the Computer	
	✓ Must use a strong complex password of at least 15 characters and do not share it. Biometric login is allowed. ✓ Must not alter the configuration of your windows computer (in case of other distribution check with iDirect IT). ✓ Computer Hard drives should be protected using whole disk encryption utilizing at minimum the AES 256-bit cipher standard. ✓ Use a digital password vault to securely store different passwords. IT can provide recommendations. Do not use the browser's built-in password manager to store passwords.
Travelling to or from work	
	✓ Protect the information on your screen, position yourself so that others cannot read over your shoulder while working. Restrict the viewing angle to reduce the risk of information being viewed by unauthorised persons during their use. Prevent others from easily reading along. ✓ Prevent others seated near you from easily reading what you are working on. ✓ Disable Wi-Fi and Bluetooth when not in use. ✓ Only take necessary data with you.
At work	

- ✓ You must apply the recommended updates.
- ✓ You must keep anti-virus software enabled unless allowed explicitly by iDirect IT.
  - ✓ Do not install additional software unless it has been through security approval. New software can be requested via a Service Desk ticket.
- ✓ Do not install additional software unless is has been through security approval. New software can be requested via a Service Desk Ticket
- ✓ You must not tamper or otherwise modify the operation of any corporate installed security application.
- ✓ Do not store data solely on the computer, use the iDirect storage mechanisms.
- ✓ Lock your computer screen when you leave your desk.

After work

- ✓ Shutdown your computer (at least weekly) and avoid putting it into sleep or hibernate. This is to make sure updates are installed.

5.4.2 Non iDirect Provided Computer (Laptop/Desktop)

Contractors or consultants of iDirect must not undertake personal endeavours while actively connected to the iDirect network. All equipment used to conduct business on behalf of iDirect will have its access revoked at any time if there is concern that the guidance in this policy is not followed, there are indicators of a data leakage or a security compromise.

iDirect requires copies of any incumbent security policies that complement or conflict with this document prior to any access being granted. iDirect may contact you to conduct posture checking of your computer to make sure it adheres to the security principles in this document and the relevant security policies of your company, depending on which are more stringent. If it is found that your computer does not adhere to your own company polices, access will be revoked pending a manual posture check of your computer. This check can be conducted verbally, written or via an interactive session if required.

You shall adhere to the following principles in this document, and contact your Local IT Team in case of a problem:

Securing the Computer

- ✓ Use a strong complex password of at least 12 characters if possible and do not share it. Biometrics for login is acceptable.
- ✓ Have current antivirus active on the computer to protect against malware.
- ✓ A firewall should be enabled to help protect against network intrusion.
- ✓ Make sure that all operating system and application updates are installed.
- ✓ Do not store iDirect data solely on the computer, use the iDirect storage mechanisms.
- ✓ Computer Hard drives should be protected using whole disk encryption utilizing at minimum the AES 256-bit cipher standard.
- ✓ Use a digital password vault to securely store different passwords. Your local IT team can provide recommendations. Do not use the browser's build-in password manager to store iDirect passwords.
- ✓ Shutdown your computer (at least weekly) and avoid putting it into hibernate. This is to make sure updates are installed.
- ✓ Try to connect to secure, password-protected wireless networks whose origin you preferably know. For example, a hotel wireless network is acceptable; however, in a bar, ask the personnel first which network is theirs.
- ✓ Lock your computer screen when you leave your desk.

Travelling to or from work

- ✓ Always protect iDirect Information from disclosure.
- ✓ Prevent others sat near you from easily reading what you are working on.
- ✓ Only take the necessary data with you.

At work

- ✓ You must apply the recommended updates.
- ✓ You must keep anti-virus software and firewalls enabled.
- ✓ Avoid installing additional software unless absolutely required, always try to validate with your IT Team.
- ✓ Do not store iDirect data solely on your computer, use the iDirect storage mechanisms.
- ✓ Lock your computer when away.

End of Contract
✓ On your last day you must remove all iDirect owned data and software from your computer after you have confirmed the data has been saved in the appropriate iDirect information store. Please work with your iDirect contact to confirm this. ✓ On your last day you must make sure that all hard copies of non-public iDirect information have been destroyed, rendered unreadable and unrecoverable.

5.4.3 Mobile devices (smartphone or tablet)

Contractors of iDirect must not access iDirect services from your mobile phone or tablet unless it's required to do your work, and you have approval from your iDirect manager.

Adhere to the following principles and contact itsecurity@idirect.net in case of a problem:

Mobile Device Security
✓ Protect your mobile device with an access code (passcode, keystroke, touch id). ✓ Keep your mobile device and apps up to date. ✓ Only install applications from the smartphone's official resources. ✓ Avoid conducting confidential conversations on public transport. ✓ Reject any Bluetooth connection request from unknown devices. ✓ Keep the device close to you and do not leave it unattended unless it is secured. ✓ Protect the information on your screen, position yourself so that others cannot read over your shoulder while working or restrict the viewing angle to reduce the risk of information being viewed by unauthorised persons. ✓ You must not store confidential iDirect data on your device. ✓ Report stolen or lost mobile devices that contain iDirect data immediately to your local IT Team and itsecurity@iirect.net. ✓ The use of Jailbroken (iOS) or rooted (Android) smartphones is prohibited ✓ Connect to secure, password-protected wireless networks whose origin you preferably know. For example, a hotel wireless network is acceptable; in a bar, ask the staff first which network is theirs.

End of Contract
✓ On your last day you must remove all iDirect owned data, software, and configuration from your mobile device.

5.4.4 Portable media (USB keys and removable disk drives)

We strongly discourage the use of Portable media, i.e., USB keys, removable disk drives. Portable media can only be used by exception. Portable media must not be used for combined professional and private purposes. If you have been instructed by your iDirect manager to use portable media It is important to adhere to the following principles:

Securing Portable media
✓ Encrypt as much as possible any portable media containing non-public iDirect information. ✓ Apply a strong password when activating encryption and store it securely. ✓ Do not use portable media from an unknown or untrusted source. ✓ Never leave portable media unsecured and unattended. ✓ Securely dispose of old portable media by returning them to IT.
End of Contract
✓ On your last day you must delete all iDirect owned data, software, and configuration from your portable device, preferably by formatting the device and removing any partitions. Please contact your local IT team for guidance on how to do this or email itsecurity@idirect.net.

6 Artificial Intelligence

Do not use any artificial intelligence (AI) tools or technologies in the creation of Work Product for the Company without obtaining prior written consent from your iDirect Manager. Disclose any intended use of AI tools and provide sufficient information to your iDirect Manager to evaluate the potential impact on the Work Product. iDirect reserves the right to approve or deny the use of such tools at its sole discretion.

- Unless you have prior approval from the Information Security department, you should never submit to a Generative AI Tool any confidential or proprietary information, data, or materials, including personal data, customer information, business plans, non-public financial information, marketing plans, source code, and anything that might be considered a trade secret. If you would not share the

information publicly, you should not use it as an Input into a Generative AI Tool. You must comply with this mandate even if you have disabled features that limit the tool provider's use of Input and/or Output or have disabled the chat history or similar features in the Generative AI Tool.

- Without prior written approval, you may not use as Input into any Generative AI Tool any third-party confidential information or trade secrets that have been disclosed to the Company by a third party. You should assume that all Input and all Output will be available to our competitors, customers, and suppliers.

- Do not use Generative AI Tools in a way that could create or result in bias (including in any decision-making process) or for any illegal or unethical purpose, such as generating malicious code.

- Do not use Generative AI Tools in a manner that might violate intellectual property laws, such as for reverse engineering or replicating copyrighted code, copying materials that could be owned by third parties or passing off Output as your own.

- Do not rely on any Output without reviewing, verifying, and testing the Output to ensure that it is accurate, error-free, appropriate, and suitable for the intended purpose. As a rule, if the output cannot be verified or confirmed through reliable sources, you should not use the Output.

7 Information Security Incident Reporting

Your collaboration and adherence are crucial. Below are examples of information security incidents that must be reported while you are under contract with iDirect:

- ✓ Loss or theft of any IT equipment containing iDirect Data.
- ✓ Suspicion of physical tampering with IT equipment when travelling (e.g., handling of device by customs).
- ✓ Abnormal behaviour of your computer or mobile device, which may be due to an attack from a hacker or the existence of malware.
- ✓ Errors in the diffusion of iDirect data: e.g., distributing customer information to wrong receivers.
- ✓ Loss or theft of any hard or soft copy documents, e.g., Document forgotten in a hotel room, USB key left on train etc.

- ✓ Tampering or notice of an attempt of tampering with IT equipment.
- ✓ Reception of e-mails on the iDirect email platform with malicious intentions (e.g., e-mail with virus attached or phishing e-mail).
- ✓ Indication of a potential security breach (e.g., logins to customer environments, outside of business hours, without a request from a customer).
- ✓ Virus detection alerts received while working under contract with iDirect
- ✓ Notice of confidential iDirect information published on a public website.

Do not hesitate to report any of the above or other unusual occurrences to your internal IT security team and the iDirect security team (itsecurity@idirect.net) within 24 hours

8 Compliance

8.1 General deviations

Some aspects of this Acceptable Use Policy could become an obstacle to perform work in general. In case a deviation is required to perform specific areas of work that are in clear contrast with this Acceptable Use Policy, the local teams who experience this must seek a policy exception that needs to be initiated by your iDirect point of contact.

8.2 Disciplinary actions

A violation of this policy by a contractor or consultant may result in termination of the agreement or removal of the contractor or consultant from an iDirect engagement. Disciplinary actions refer to actions or penalties taken in response to negligence or intentional non-compliance with this Acceptable Use Policy, including, but not limited to, theft, intentional destruction or leakage, spreading of iDirect data, willingly allowing espionage to occur, and/or willingly sharing confidential information with unauthorized persons. All disciplinary actions will be taken in compliance with local law and local employment regulations.

9 Revision Management

9.1 Document Change Log

The full version history of this document is also part of the metadata of this document stored in the DMS.

Revision	Changes Submitted By:	Summary of Changes
2	Craig Barnfield	*Document Classification Change* *Internal Use Only > Public.* *Section 2,* *Updated scope language.* *Section 4,* *Added a requirement to complete all assigned training to maintain access to the iDirect network* *Specified that travel with iDirect confidential data is not allowed, except as per Section 5.4.1* *Added a requirement to request additional permissions, system access, software, and VPN updates via the Service Desk ticketing system* *Clarified that only software that has been security reviewed and approved can be installed on iDirect systems* *Stated that only the iDirect VPN can be used to connect to the iDirect network, and any unapproved remote access methods will result in disciplinary action* *Section 5.2,* *Clarified that confidential information must be encrypted when sent outside of iDirect's communication systems.* *Added a restriction on using the iDirect email account for private usage or any usage not directly* *Specified that email forwarding rules that forward internal emails externally require explicit permission from itsecurity@idirect.net* *Section 5.4,* *Emphasized that corporate data must only be stored on supplied tools of iDirect and not solely on the computer's hard drive*

		Section 5.3, *Stated that the usage of anonymizing services (e.g., private VPN, Tor browser) is prohibited while working on or connected to iDirect resources* *Section 4 & 5.4.1,* *Added a requirement for contractors or consultants to request new software via a Service Desk Ticket.* *Clarified that personal or private computers can only be used with approval from the iDirect manager.* *Section 5.4.3,* *Specified that contractors must not access iDirect services from mobile devices unless required and approved by the iDirect manager.* *Section 5.4.4,* *Stated that portable media can only be used by exception and must not be used for combined professional and private purposes.* *Section 9,* *Added change table.* *Updated Reviewers and approvers.*
2	Craig Barnfield	*Minor grammar updates throughout.* *Updated 9.2 Review & Approval Responsibilities*

9.2 Review & Approval Responsibilities

Function	Responsibility
Information Security Manager	Author / Owner
ISMS Officer	Reviewer
VP Corporate Compliance	Approver
Director Global Perfromance	Reviewer
VP Senior Fellow Engineering, Global Engineering	Approver
Responsibilities = Author, Owner, Reviewer(s), and Approver	

Review and approvals are electronically maintained in the DMS.