IS01 - Information Security Policy

Agile Content Group

Document History

Version	Date	Reviewer	Changes
1.0	2022	Legal Team	Initial Document
1.1	March 2023	Legal Team	Add Do's and Don'ts
1.2	April 2025	Information Security Team	Alignment with new policies, some corrections to definitions.

Summary

Overview

Agile Content is committed to protecting Agile Content's employees, customers, partners, end-users and Agile Content internal information from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internally, the internet/intranet/extranet systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts, providing electronic mail, internet browsing, file transfers protocols and physical documentation are Agile Content's property. These systems and documentation are to be used for business purposes in serving the interests of Agile Content, and of our clients, customers, and partners.

Effective information security is a team effort involving everyone in Agile Content who deals with and has access to information, whether digital or in physical format, and/or information systems. It is our collective responsibility to know these requirements, and to conduct ourselves accordingly.

These requirements are in place to protect Agile Content's employees and Agile Content clients and partners. Inappropriate use exposes Agile Content to risks including virus attacks, proprietary, confidential, personal data theft and misuse, compromise of network systems and services, legal issues, and reputational damages.

This Policy applies to all Agile Content contractors, consultants, and employees (including system support staff with access to privileged administrative passwords and senior leadership with access to restricted and confidential information).

Purpose

The purpose of this Policy is to provide all Agile Content contractors, consultants and employees with information to secure the use of information, physical documentation, electronic and computing devices, network resources, internal networks, and business systems, whether owned or leased by Agile Content, the employee, or any third party. All employees, contractors, consultants, temporary and other workers in Agile Content are responsible for exercising good judgment regarding appropriate use of information in accordance with Agile Content requirements, policies, standards, and legal and regulatory requirements, including the General Data Protection Regulation (GDPR) and Network and Information Security Directive 2 (NIS2).

Acting

Agile Content employees, consultant and contractors, in their day-to-day dealings may have access to confidential and/or restricted information which must remain secure and protected. It is the responsibility of every Agile Content employee, consultant, and contractor to ensure that the information accessed, handled, or created remains secure and protected.

This means employees are required to:

- Recognise what information must be kept protected and confidential and pay special attention to types of information which could cause harm if lost, stolen, or destroyed.
- Following all formal policies and procedures and ensuring that legal requirements and regulatory, including GDPR, requirements are met.
- Follow the best practice behaviours and requirements outlined in this presentation.

- Inform managers of information security discrepancies or vulnerabilities they believe exist in people's actions, operational or administrative processes or implemented technology (without attempt at exploitation).
- Using common sense and professionalism.

Please carefully read and apply all information and requirements in this document, including the information which follows. If you have questions, please contact the IT Team (**it-team@agilecontent.com**), who will assist you.

Information Security

All non-public data and information which you access, create or handle, needs to be secured and protected. The following are descriptions and requirements of the general categories of data and information which you might access, create, or handle.

- Business and Operational Information: This information includes both our internal information - which gives us our competitive edge and that of third parties which we are/were in business dealings (e.g. products, business plans, client lists, financial information, price lists, policies and procedures, inventions, know-how, ideas, marketing information, strategy plans, corporate organisational charts, various forms of intellectual property including source code, trade secrets, and every non-public information). It is our duty – your responsibility - to protect not only our internal information, but also the information of every third party.
- Third Party Information: All non-public partner, customer, or vendor information that we hold such as employee names and contact information, order details and other business and operational information, intellectual property, and each non-public information whether in digital or physical format.

- Personal Data (Information): Refers to any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Therefore, this includes all employee information as well as information we hold and/or have access relating to customers, partners, vendors, end-users, amongst others.
    - Regulatory Rights: In some locations, including, but not limited to, the European Union under the General Data Protection Regulation ('GDPR'), data subjects have specific rights related to their personal data. Accordingly, as a data processor or controller, Agile Content employees, contractors, and consultants need to be aware of these rights and be able to timely respond in accordance with lawful practice.
        - Right to be informed: When data subject requests information on their data we have a duty to respond.
        - There are a few other rights that may trigger responsibilities from Agile Content employees, contractors, and consultants (some rights are curbed by respective rights of Agile Content):
            - Right to Access, Rectification and Erasure of Data
            - Right to Restrict Processing
            - Right to Data Portability
            - Rights related to Automated Decision Making

- Agile Content employees shall thoroughly comply with personal data protection law in their jurisdiction, the laws that apply based on the processing of personal data that they carry out and the laws determined by binding rules or resolutions adopted within the Agile Content Group.
- Agile Content employees must also strive to ensure that the principles set forth herein are complied with.
- The main principles relating to the processing of personal data must be always observed. The principles are described below:
    - **Principle of legitimate, lawful, and fair processing of personal data.**
        - The processing of personal data must be legitimate, lawful, and fair, in accordance with applicable law. In this sense, personal data must be collected for one or more specific and legitimate purposes, in accordance with applicable law.
        - When so required by law, the consent of the data subjects must be obtained before their data are collected.
        - Also, when required by law, the purposes for processing the personal data shall be explicit and specific at the time of collection thereof.
        - In particular, Agile Content employees shall not collect or process personal data relating to ethnic or racial origin, political ideology, beliefs, religious or philosophical convictions, sexual orientation or practices, trade union membership, data concerning health, or genetic or biometric data for the purpose of uniquely identifying a person, unless the collection of said data is necessary, legitimate and required or permitted by applicable law, in

which case they shall be collected and processed in accordance with the provisions thereof.

- **Principle of minimization.**
  - Only personal data that are strictly necessary for the purposes for which they are collected or processed and adequate for such purposes shall be processed.
- **Principle of accuracy.**
  - Personal data must be accurate and up to date. They must otherwise be erased or rectified.
- **Principle of storage duration limitation.**
  - Personal data shall not be stored for longer than is necessary for the purposes for which they are processed, except in the circumstances established by law.
- **Principles of integrity and confidentiality.**
  - Personal data must be processed in a manner which is compliant with Agile Content technical or organizational measures to ensure appropriate security that protects the data against unauthorized or unlawful processing and against loss, destruction, or accidental damage.
  - The personal data collected and processed by Agile Content employees must be stored with the utmost confidentiality and secrecy, may not be used for purposes other than those that justified and permitted the collection thereof, and may not be disclosed or transferred to third parties other than in the cases permitted by applicable law.

- **Principle of proactive responsibility (accountability).**
  - Employees shall be responsible for complying with the principles as set forth herein and those required by applicable law and must be able to demonstrate compliance when so required.
  - To assist employees, Agile Content shall perform a risk assessment of the processing carried out in order to identify the measures to apply to ensure that personal data are processed in accordance with legal requirements. When so required by law, Agile Content shall perform a prior assessment of the risks that new products, services or IT systems may involve for personal data protection and shall adopt the necessary measures to eliminate or mitigate them.
  - Employees who process personal data must maintain a record of activities in which they describe the personal data processing that they carry out in the course of their activities.
  - In the event of an incident causing the accidental or unlawful destruction, loss or alteration of personal data, or the disclosure of or unauthorized access to such data, employees must immediately report it (within a maximum 48-hour window) using the specific form available in our helpdesk portal. Such incidents must be documented, and measures shall be adopted to resolve and mitigate potential adverse effects for data subjects.
- **Acquisition or procurement of personal data.**

        - It is expressly forbidden for Agile Content employees to purchase or obtain personal data from unlawful sources, from sources that do not sufficiently ensure the lawful origin of such data or from sources whose data have been collected or transferred in violation of the law.

    - **Engagement of data processors.**
        - Prior to engaging any service provider that may have access to personal data for which Agile Content Group companies are responsible, as well as during the effective term of the contractual relationship, Agile Content employees must adopt the necessary measures to ensure and, when legally required, demonstrate, that the data processing is performed in accordance with applicable law.

    - **International transfers of data.**
        - Any processing of personal data that is subject to European Union regulations and entails a transfer of data outside the European Economic Area must be carried out strictly in compliance with the requirements established by applicable law in the jurisdiction of origin. In addition, Agile Content employees located outside the European Union, who handle, process, or have access to personal data, must comply with any requirements for international transfers of personal data that are applicable in their respective jurisdictions.

- Please contact Agile Content Legal Department in the event a question may arise as to these types of rights. Also see Agile Content Privacy Policies

- Other Data: Information security also refers to other personal, proprietary, and confidential data stored both in databases, storage devices as well as data contained in physical documents (whether internal or regarding third parties), namely, but not limited to, contractual documentation. Therefore, to ensure the data is kept secure and protected, data should be stored safely, using proper access control as defined in our internal policies.

Typical fraudulent schemes

Any action our company undertakes that involves coming into contact with, processing or storing personal, proprietary and confidential data must be done with the highest standards of security in mind at every step. Whether you are accessing, processing, or storing internal or external data, such as employment contracts, employee personal data, internal proprietary data, confidential data, financial data, third party contracts, third party personal data, proprietary data, confidential data, banking data, amongst others, you must uphold the strictest care and attention to protect such information at all times.

There are several schemes' individuals may use to access secured data for fraudulent activities and personal gain. The most common scheme to obtain internal/external information for fraudulent activities arise from phishing schemes, which originate in e-mail and communication services where an outside third party poses as either an internal employee or an external customer, client or partner employee in order to obtain information and/or circumvent security policies, for personal gain.

It is **key** that every employee understands that requests such as, but not limited to, passwords, banking account information, solicitations to alter customers banking transfers, purchase requests, amongst others should be dealt with extra care and attention. Therefore, every request that represents an alteration to a day-to-day procedure, banking information, password information, amongst others must **always** be double checked with managers and the related customers, **using a new e-mail chain** or other means of communication, to ensure the request is valid and authentic. But remember, there are always new ways and schemes used by individuals to execute fraudulent activities.

Other common fraudulent example scheme occurs by telephone where an individual requests your email to send you some service information. Never open emails from unknown sources and never click on unknown links inserted in e-mails you receive from unknown sources. Please see below some other examples:

- **Phishing:** In this type of attack, hackers impersonate a real company to obtain login credentials. Users may receive an e-mail asking to verify their account details with a link that takes them to an imposter login screen that delivers their login information directly to the attackers.
- **Spear Phishing:** Spear phishing is a more sophisticated and tailored phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use a real username and phone number and refer to Agile Content in the e-mail to trick users into thinking they have a connection with them, making them more likely to click a link or attachment that they provide.
- **Whaling:** Whaling is a popular ploy aimed at high profile members of the company, with the ultimate goal of getting access to higher privileged accounts that have access to more sensitive assets, bank accounts or confidential information.
- **Shared Document Phishing:** Users may receive an e-mail that appears to come from file-sharing sites like Dropbox or Google Drive alerting them that a document has been shared with them. The link provided in these e-

mails will take a user to a fake login page that mimics the real login page and will steal his account credentials.

What you can do

To avoid these schemes, users should observe the following practices:

- Think before you click: do not click on links or attachments from senders that you do not recognize (hover over links that you are unsure of before clicking on them). Be especially wary of .zip or other compressed or executable file types. We have multiple layers of protection in place, but sometimes, bad actors find ways to slip some of these though all of them.
- Do not provide sensitive information (like usernames, passwords, credit card numbers or banking information) over email / phone.
- Always double check with managers and the related customers, using a new e-mail chain, or preferably, other means of communication, to ensure any financial or banking information alteration and/or request is valid and authentic.
- Watch for email senders that use suspicious or misleading domain names. Please see some common examples:
    - John Doe <John.doe@ag1letv.com>
    - John Doe <John.doe@br_agiletv.com>
    - John Doe <John.doe@pt_microsoft.com>
- Inspect URLs carefully to make sure they're legitimate and not imposter sites (check tools at the end of this document).
- Do not try to open any shared document that you're not expecting to receive.

- If you can't tell if an email is legitimate or not, please contact the IT Team (**it-team @agilecontent.com**).
- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.
- Keep your computer operating system as well your applications (including web browsers) up to date with latest security updates and patches.
- Keep your anti-virus/anti-malware running.
- Keep your local firewall active.
- Attend the company provided security awareness pills.
- In case you received an e-mail with a phishing scheme, please report it using the Information Security Report form in the helpdesk portal.

The Do´s and Don'ts

Recommended actions

- Delete spam, chains, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Do not allow direct disk sharing with read/write access unless there is a mandatory business requirement to do so.
- Always scan disks, external hard-drives and similar removable media from an unknown source for viruses before using it.
- NEVER give passwords, banking/financial information, accept requests for banking transfers alteration without double checking the information to ensure it is trustworthy and authentic.

- NEVER engage in purchases directly even if the request comes from your manager or any hierarchical superior (up to the CEO) without double checking the information to ensure it is trustworthy and authentic.
- NEVER convey or transmit personal information lists to third parties outside Agile Content or outside the scope of contractual engagements our company is bound to.

Prohibited actions

- The following activities are strictly prohibited, with no exceptions:
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Agile Content.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Agile Content or the end user does not have an active license.
- Accessing data, a server or an account for any purpose other than conducting Agile Content business, even if you have authorized access.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password or allowing use of your account is expressly prohibited – this includes access to other Agile Content employees, family and other household members when work is being done at home.
- Using an Agile Content computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/intranet (One Agile)/extranet.

Email and communication activities

- Circumventing user authentication or security of any host, network or account.

- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding “chain letters”, “ponzi” or other “pyramid” schemes of any type.

Employee responsibilities

- Passwords: make sure that you keep your password confidential and do not share your login details with anyone else.
- Locking your desktop: your computer should do this automatically after 15 minutes of inactivity, but it’s always good practice to lock your desktop before walking away from your desk to make sure any Information you have on the screen isn’t seen by someone else.
- Being aware of virus software: take care when opening emails and attachments or visiting new websites you’re not familiar with – they could download viruses to your computer which could cause an Information breach. If you believe you’ve been sent an email with a virus or accessed a website which could have provided a virus access to your computer, notify IT Team immediately.
- Email etiquette:
    - the email recipient auto-populate function can be a useful tool but always double check that the correct address has been selected. It’s all too easy to send the right Information to the wrong recipient but sometimes the damage cannot be undone.

  - Employees should be careful when using the email forwarding function – make sure you're never forwarding inappropriate Information, such as sensitive, confidential and/or Personal Data to someone who does not need to see it.
  - Employees should also make sure never to send Information accessed as part of their job to a personal email address.

- Portable media: if you need to save Confidential Information or Personal Data on removable, portable media, make sure the removable media is password protected or encrypted before you take it with you. Never use 'found' portable media devices (USB drives, etc). These have been used in the past as the catalyst to major security breaches around the world.
- Disposal of Confidential Information: Most office locations have an on-site confidential waste bin which is regularly emptied and securely disposed of by a third party. Any paper materials you have which have Information on them and need disposal should be placed in confidential waste bins only and not in the normal rubbish bins. Alternatively, if you do not have access to such bins at your office, if disposal of confidential information is a regular occurrence discuss this with your manager to determine if a disposal service is appropriate. In any event, confidential Information should be shredded ahead of disposal.
- Returning Information to filing cabinets: if you need to access hard copy information stored in filing cabinets, make sure you return it to the filing cabinet once you've finished using it.
- 'Clear desk' working we try to maintain a clear desk type approach to working – make sure all documents containing Information are stored away when you're away from your desk and that your desk is clear of documents before you go home each day.

- Using shared systems: Some systems we use have free text fields where users can input additional information of their choosing, e.g. Salesforce.com. These fields should never be used to record non-business-related Personal Data or any other sensitive or Confidential Information of any kind.

- Someone asking about their data: sometimes a third party may contact you to ask about the information we hold about them. If you receive a request like this, please forward it to the Legal Team at legalteam@agilecontent.com as soon as possible for review, so we can check its legitimacy and respond accordingly.

- Update records: if somebody tells you that some of their data has changed, make sure you update it in the relevant system promptly. If you have any Personal Data you no longer need, i.e., the purpose is no longer active, make sure you take steps to delete it following the data disposal procedures. If the data refers to banking and/or financial information, never assume it is correct, always double check through a new email chain and confirm its validity.

- Visitors: always ensure any visitor into the building has signed in at reception and is always accompanied when in the building (or as far as is reasonable).

- If required, confidential or commercially sensitive documents should be password protected or maybe even the laptop hard drive encrypted.

- Internal Policies: make sure you comply with all Agile Content policies, which can all be found on Bamboo, as well as the confidentiality provisions in your employment contract, as applicable.

- Vigilance: there are people who will try and trick you to give them Information – either via email, post or over the phone. Always ask for additional clarifications to confirm the request is legitimate and never disclose Information where you're not sure. If in doubt, ALWAYS refer the request to the Legal team.

- Professionalism: Employees should especially take care and not send offensive emails about other people, their private lives or anything else that could bring Agile Content into disrepute. Employees should also take care not to save any inappropriate Personal Data to their work computers or folders on the Agile Content network.
- IT Assets Usage: IT assets must only be used in connection with the business activities they are assigned and / or authorized.
- IT Assets Classification: All the IT assets must be classified into one of the categories in the Organization's security categories; according to the current business function they are assigned to.
- User Responsibility: Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
- IT Assets Prevention: All the IT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the aforementioned assets.
- IT Asset Access: Access to assets in the Organization location must be restricted and properly authorized, including those accessing remotely. Company's laptops, PDAs and other equipment used at external location must be periodically checked and maintained.
- IT Assets Care: Special care must be taken for protecting laptops, PDAs and other portable assets from being stolen. Be aware of extreme temperatures, magnetic fields and falls. Losses, theft, damages, tampering or other incident related to assets that compromises security

must be reported as soon as possible to the Information Security Team using the Information Security Report procedure.