GDPR COMPLIANCE

SUMMARY OF TAKEN MEASURES AND ANSWERS TO FREQUENT QUESTIONS

March 31st 2018

Patrick Mareuil
Chief Innovation Officer
+33 1 44 56 87 14
pmareuil@accengage.com

Nicolas KLAIN
CFO & DPO
+ 33 1 44 56 87 12
nklain@accengage.com

I. INTRODUCTION TO GDPR

I.1 Scope of GDPR

The General Data Protection Regulation (GDPR) was approved by the EU Parliament on 14/04/2016 and will be **enforced on 25/05/2018**.
It replaces the Data Protection Directive 95/46/EC and was designed to **harmonize data privacy laws across Europe**, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

The scope of the GDPR is **any processing** of **Personal Data** from **EU data subjects** (ie users based in the EU).
This means **increased Territorial Scope** (extra-territorial applicability). Indeed the GDPR applies to all organizations/companies processing the personal data of **data subjects residing in the Union**, **regardless of the company's location**. In other words, a company based outside of the EU but processing personal data of EU residents will be required to abide by GDPR.

A key change to previous regulations is **increased penalties & co-responsibility**: under GDPR, organizations in breach of GDPR can be fined up to 4% of annual global revenues or €20 Million (whichever is greater).
It is important to note that these rules apply to both **Data Controllers** (the company which owns the data, ie you, the Accengage customer) and **Data Processors** (the company which processed data on behalf of the Data Controller, ie Accengage).

I.2 Personal Data & Consent

Due to the definition of Personal Data and further statements on online identifiers, it is safer to consider that the **data which are collected via Accengage tools** on behalf of Data Controllers are **personal data**.
Definition of Personal Data is given as *"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,** in particular 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"*.
Further statements are made regarding what should be considered Personal Data: "***online identifiers** provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or **other identifiers***", which "*may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and **identify them***".
As a consequence, due to the fact that mobile or web identifiers can be related to account or customer identifiers, and therefore to an identified person, the data collected by Accengage tools should be **treated as Personal Data.**
GDPR is therefore applicable to the data processed by Accengage on behalf of their Data Controller.

Although other legal basis for processing might be invoked (such as legitimate interest of the controller – including direct marketing –, context of a contract etc.), **Consent of the user** is the **main legal basis for the processing to be lawful**.
As a consequence, companies should seek a **clear, freely given, unambiguous and informed Consent** from their users prior to processing (including collecting) personal data. "*Silence, pre-ticked boxes or inactivity*" are explicitly cited as not constituting consent.
It must be as easy to withdraw consent as it is to give it

I.3 GDPR Principles and processes

The GDPR enumerates **several principles** which should be taken into account, including:

- **Data Protection by Design** – since the **design** of the processing (in our case of our software), one should have data protection in mind and act in order to identify personal data at stake, minimize such data, protect it and have transparency
- **Data Protection by Default** – the processing should only involve personal data which is **necessary for its purposes** and should limit data collection and processing to it
- **Accountability** – the Data Controller should be able to **demonstrate at all time its compliance** to these principles (as opposed to be able to correct it once there is a warning, in previous regulations) and processes…

The GDPR also cites **specific processes** to abide by (such as maintaining records of processing, appointing a Data Protection Officer, having a communication in case of breach…), and states that companies should **take appropriate organisational and technical measures** to ensure Regulation requirements and data security.

Finally the GDPR has extended some rights of the **users**:

- Right to be informed - your users need to be told what data are collected about them and for what purpose.
- Right to Erasure & Right to Object – your users may request that their data be deleted and that their data no longer be processed.
- Right of Access/Right to Portability – your users may request to have access to their data
- Right to Rectification – your users have the right to rectify their personal data if it is inaccurate or incomplete.

II. ACCENGAGE & GDPR

In this part, we will see what measures Accengage has taken to help you comply with GDPR.
As the **European leader for Push Notifications**, Accengage has always undertaken 'European-standards' measures (whether technical or organisational) to maintain a high level of data protection, user privacy and software security and as a consequence complying with the GDPR was facilitated.
Accengage is **counselled by the Law Firm *'Staub & Associés',* specialised in Intellectual Property, digital and IT,** which audited Accengage practices, established recommendations and organized workshops.

II.1 Role & Data ownership

Accengage acts as a **Data Processor** on your behalf, and you, as owner of the mobile app or website, are the Data Controller.
Very simply, Accengage does not hold any ownership of the user data processed on behalf of the Customer.
Accengage may only derive benchmark performance data on **anonymous basis** and per industry, if the statistics cannot be attributable to a given customer nor user (every year Accengage publishes a benchmark on the performance of Push Notifications, on an industry level, i.e. overall statistics per industry, an example of the benchmark can be found here: https://www.accengage.com/infographic-opt-in-and-reaction-rates-of-push-notifications-for-mobile-apps-websites-and-facebook-messenger).

II.2 GDPR compliancy in a nutshell

In order to help you comply with the GDPR and its application in May 2018, Accengage has already taken or is taking numerous measures:

- Accengage provides **multiple technical methods** in its software to enable you to **fulfil requirements** regarding user consent and user rights, such as: collecting proof of user consent and dates, providing user data for modification, erasing user data if need be etc.
- Accengage has taken **technical and security measures** to protect and minimize user data, hence respecting Data Protection by Design and Data Protection by Default principles (confirmed by the results of numerous audits and penetration tests, which can be accessed upon request)
- Accengage has located all **storage of personal data inside the European Union**
- Accengage has taken **organizational measures** to ensure high level of data protection (staff training & awareness program, clauses in employee contracts…)
- Accengage has appointed a **Data Protection Officer** within the company
- Accengage has an **Incident Management** and **notification Plan** in case of a Breach
- Accengage signs **Data Processor Agreements** with its customers and maintains records of processing activities (although it is under 250 employees).

II.3 Consent & User rights

As the Data Controller, you should **seek your Users consent** before processing their data in your mobile application or website.
The GDPR and Working Party 29 have given indications on how to proceed.
User Consent as it is stated must be '***freely given, specific, informed and unambiguous',*** with ***'a clear affirmative action'***. "*Silence, pre-ticked boxes or inactivity*" are explicitly cited as not constituting consent. Likewise, it cannot simply be a paragraph within terms and conditions.

As a consequence, a good way for seeking consent would be through for instance a Pop-up/AlertBox informing the User about the various data processing occurring, the type of data processed and their purposes.

The Accengage software on client side (SDK, Javascript…) should be **launched once user consent has been granted**.
However a new version of the SDK in April will allow you to minimize impact on development, and to simply inform the software when user consent is granted, without having to delay the launch of the SDK (the SDK suspending automatically all processing while consent has not been collected).
Accengage will collect when a user consent is given, and the **dates** and **sources** for that consent, to **facilitate the proof of that consent for you.** Indeed under GDPR, the Data Controller should be able to demonstrate user consent.
The Accengage software has also always provided a DoNotTrack method which enables you and the user to suspend data processing and software execution for a user. This method can be integrated as a switch for the developer for instance. Under the new version, this method will be unified with the new method for user consent.

Accordingly to GDPR, users benefit from certain rights and Accengage provides technical methods to enable you to fulfil these rights:

- **Right to Object** ⇨ the DoNotTrack SDK method allows to the user to withdraw consent from data processing, from within the app
- **Right to Erasure** ⇨ Accengage will provide in May the possibility via an SDK method and REST APIs to flag and delete users who wish to have their data erased (on top of the automatic purge mechanism – see below). In the meantime, it is possible to erase user data by providing the device ID of the user who wishes to erase its data
- **Right of Access/Right to Portability** ⇨ Accengage provides REST APIs to read and export user data
- **Right to Rectification** ⇨ Accengage provides SDK methods and REST APIs to modify data user

Also Accengage has always provided a **purge mechanism** to **anonymize or erase** user data after **12 months of inactivity** (based on last open date) or after 3 bounces recorded, in order to fit proportionally with the purpose and extent of data processing, hence respecting the Data Protection by Default principle (the data processing may last as long as the app is installed on device for instance). This mechanism can be amended (shortened) based on specific requests by the Customers.

II.4 Data collected

Once User Consent has been granted, the Accengage software will be launched and will proceed with data processing.
Accengage provides a **list of data collected in the Appendices**, and distinguishes between automatically and mandatory collected data, automatically but optional collected data, and data that you as the developer and Data Controller may wish to tag and collect. The data collected include:

- Data used to identify the Device (for the functioning of Push) such as Device ids, Push Notification Token…
- Device Characteristics (for targeting): Device Language, country code, OS version, app version, device model, connection type
- Visit information: Number of visits, install date, last open date
- Campaign information: Sent campaigns, clicked campaigns
- As options: Geolocation (if activated), Geofence entered (if activated), Events tagged by customer, User Profile information tagged by customer…

Accengage prevents in its terms and conditions to tag and host “specific user data” (formerly known as sensitive data), such as political or philosophical views, medical data, sexual orientations etc.

II.5 Data storage & Data separation

All data are hosted are **stored in the European Union**, in 2 Datacenters: the main one in Paris area (St Denis – France – managed by Claranet, a major and recognized player of Managed hosting services, positioned as a Leader in Gartner Magic Quadrant since 2013, with offices in UK, France, Germany, Spain, Portugal, Benelux) and the second one in Brussels (Belgium –Google Cloud Europe).

The Accengage platform has been audited and approved by many large corporations with high-level of demand (AXA, BNP Paribas, the French National Lottery, Solocal/PagesJaunes Group, Voyages-SNCF...).

Accengage delegates to Claranet the management of the hosting infrastructure.
Claranet is **certified**:

- ISO 9001 (Quality management systems)
- ISO 27001 (Information Security Management systems)
- PCI-DSS (Security for the payment account data protection)
- ITIL (Information Technology Infrastructure Library)
- ISO/IEC 20000 (the first international standard for IT Service Management).

Claranet certifications are detailed on: http://www.claranet.co.uk/about-us/accreditations-and-technical-partners (additional certifications are available on local websites from Claranet).

The servers from the main Datacenter are hosted in the **Datacenter Equinix Paris (PA2)**:

- Localized in France, Saint-Denis (Paris suburb)
- complies to SSAE16 (Statement on Standards for Attestation Engagements)
- certified ISO 9001 (Quality management systems)
- certified ISO 50001 (Energy management systems)
- certified ISO 27001 (Information Security Management systems)
- certified PCI-DSS (Security for the payment account data protection).

The Google Cloud Europe platform based in Brussels is certified:

- SSAE16/ISAE 3402 Type II, SOC 1, SOC 2 and SOC 3
- ISO 27001 (Information Security Management systems)
- ISO 27017 (Cloud Security)
- ISO 27018 (Data Protection on the Cloud)
- PCI-DSS (Security for the payment account data protection)
- ENS - Esquema Nacional de Seguridad for Spain (https://cloud.google.com/files/GoogleCloud-CertificadoENS2017.pdf).

Google Cloud Europe certifications are directly available online: https://cloud.google.com/security/compliance?hl=en.

Paris site is organized into security zones.

- **Access process**: CLARANET team and clients must comply with defined process. The welcoming visitors also follow a formal procedure which records are periodically audited. This procedure ensures that each person outside the company entering the premises is clearly identified, that person is accompanied by a CLARANET employee who is then responsible for it and all information associated with the visit are recorded in a register.
- **Site access**: 3 access levels – checkpoint, identification at the front desk and access door to the data centre.
- **Human**: security agents on site, 24/7/365.
- **Electronics**: 24/7 video control, card reader with individualized authorizations, biometric controls, registered access card and intrusion detection. Video monitoring system and motion sensor allow detecting any attempt to break in real time. Surveillance videos are stored for 30 days on Hard Drive.
- **Site security**: limited access to technical rooms, card readers at each door access.
- **Fire detection and extinction:** Claranet benefits from fire detection and extinction systems in their Data Centres. These systems can operate without damaging electronic devices. The fire detection system is equipped with VESDA (Very Early Smoke Detection Apparatus) which samples the air constantly for multiple seconds. This systems interacts with the regular fire standard detection systems and proceeds whenever 2 sensors reach alert thresholds, hence avoiding false alarms and yet enabling reactive trigger in case of fire.
- **Power supply system:** our Data Center is equipped with a redundant N +1 power system, including a UPS (Uninterruptable Power Supply) capable of providing enough power capacity for the Data Center full load. In case of malfunction of electricity arrival, UPS provides the electricity needed to operate the Data Center to Electricity Supplier recovery services.

Here are some of the **Security measures** taken by Accengage to ensure maximum security for its platform:

- The Accengage platform is protected by a dedicated Juniper type Firewall and Antivirus
- Database servers are placed in a private network unreachable from the outside

- Patch management policy is applied
- Virus DAT File updated within 1 day
- Implementation of the policy of least privilege
- Limitation of services (network and system) and application
- Equipment redundancy
- Implementation of the main countermeasures proposed by OWASP against the 10 main vulnerabilities of Web Applications (data injection, bad management of sessions and authentications, XSS, CSRF...)
- Control and encoding of all data and parameters which are sent by the devices. The implementation is executed thanks to a dedicated library (OWASP ESAPI). All expected data input are typed/normed.
- Inspection and analysis of the content of all files which are sent by Customers by anti-virus. Accengage uses a white-list which only accepts files that have a content which is non-executable, and a blacklist that prevents any executable file
- Data Backup
- Database monitoring to detect errors and prevent interruptions
- Ability to encrypt the data stream
- Training and staff awareness of data security

An Intrusion Prevention System has been implemented on the platform. This systems enables to identify:

- Known attacks based on "patterns"
- Unknown or not "patterns" attacks
- Attacks using interactive traffic (backdoors, worms, Trojans)
- Attacks overloading a resource (Sync Flood)
- Attacks on making a spanning multiple connections
- Attacks using application-level ambiguities or transportation
- Recreational attacks
- Network attacks (ARP, IP Spoof)

These are the main security mechanisms used to avoid DDoS and DoS attacks:

- Juniper Firewall hardware
- Protection of the Infrastructure against DDoS attacks (ABEL, based on a Arbor Networks hardware solution)
- Concurrent access limitations
- IP filtering to limit severity
- Cleaning center (proxy) implementation
- Load shedding for suspicious inbound traffic.

In order to have physical access to servers, Accengage personnel must:

- schedule a visit to the Datacenter 48 hours in advance with Claranet
- have Claranet, as well as Accengage CTO, approvals
- be accompanied by a Claranet staff member during the visit and follow the specified procedure.

Additionally, all Accengage hardware are secured in a cage-type container, locked with a key.

All aspects for Server, Network, Database software, OS support & maintenance are covered by the contractual agreement with Claranet, which include commitments on:

- Platform availability
- Network performance
- Incident Response Plan.

An Information Security Assurance Plan is setup, part of the agreement between Accengage and Claranet, and is reviewed on a yearly basis. Confidentiality, Responsibility and Privacy clauses are part of the Accengage and Claranet agreement.
The Information Security Assurance Plan describes:

- The requirements : access controls, information security, security linked to operations, security incident management, business continuity and audit
- The organisation put in place to meet these requirements (the security representatives, the steering committees…)
- The security measures (monitoring committee, hosting, human resources, network and data exchange, access controls, external audits…)
- Monitoring and supervision
- Data Backup and retention policies
- Security incident management procedures.

In the event any subcontractor would potentially intervene on data (data hosting, maintenance, support…), they are required to detail data protection measures and contractually to abide by GDPR standards.

We implement a Full Snapshot once per day (15-day retention) combined with a differential backup every 15 minutes. Backups are automatically encrypted and transmitted to a second Datacenter, using a dedicated and secured line. This platform backup is supervised and managed 24x7 by our engineering teams to host, identify, isolate and resolve any incident or loss of performance.

Accengage offers a multi-tenant SaaS technology. However all customer databases, environments (dev, staging and production) and data are compartmentalized from each other which prevents from other users access. All data coming from SDK or APIs are identified by application credentials (app login and private key), and all access to the User Interface are individualized, with each profile having a certain limit of rights on specific applications.

II.6 Software security and Data Protection by Design

II.6.1 Software development security principles

Accengage Products are developed with methodologies at the forefront of security standards and are secured through the following:

- SSL-secured User Interface
- All communications between SDK and servers are secured with SSL protocol and managed by REST APIs with temporary token authentication
- SSH protocol for File transfers (sFTP) or VPN are put in place when interconnection with Customer systems
- Access to application secured through login and passwords which are created and managed (several types of rights can be granted) by the customer local administrator
- Accengage provides many SDK and API methods to safeguard user rights, such a “DoNotTrack” feature which enables a developer or user to switch off the use of the SDK locally, a method to access or export user data etc
- Many different components to the SDK can be switched off remotely or suspended in case of a bad integration or any other reason
- All data and parameters which are sent by the devices are controlled and encoded. The implementation is executed thanks to a dedicated library (OWASP ESAPI). All expected data input are typed/normed.
- The content of all files which are sent by Customers is inspected and analysed by anti-virus. Accengage uses a white-list which only accepts files that have a content which is non-executable, and a blacklist that prevents any executable file.
- Scripts for exports contain validation processes to ensure consistency of data and expected format.
- iOS Push Certificates on servers are secured by a password which is stored encrypted (SHA-2) and obligatory
- User Access are secured by a password which is stored encrypted (SHA-2) and managed by ACL
- Local stored data on device is encrypted with AES256 protocol
- All customer databases, environments (dev, staging and production) and data are compartmentalized from each other which prevents from other users access
- Before starting to use any new Development Framework, a security analysis and the approval of the IS Security Manager and Chief Security Officer is necessary.

II.6.2 Encryption

Communication flows

All communications between SDK and servers can be secured with SSL protocol and with token authentication. The REST API methods are secured with SSL protocol as well as token authentication.
The Accengage User Interface is SSL-secured.

File exchanges

Imported or exported data, in the form of files, are transmitted and stored on secure SFTP (openSSH solution) servers. These files are not encrypted, but they can be on your request (OpenSSL solution).

Database

The data in the database is not encrypted, with the exception of passwords associated with user profiles and Push Notification certificates. Local data stored on the device is AES256-encrypted.

II.6.3 Security testing

The platform has been audited and approved by many large account customers (such as AXA, BNP Paribas bank, Orange…) and independent Security companies on the following items:

- Overall security policy of the company
- Penetration testing
- ID patch level: security patch missing in the System Application Framework and third components: buffer overflows, known vulnerabilities (CVE, Exploit- DB, etc.)
- Configuration errors: directory listing, insecure administration interface , prediction and login sessions
- Tests forms authentication : Accounts trivial or default Brute Force
- SQL Injection and Blind SQL Injection
- Remote and Local File Inclusion
- Reflected Cross-Site Scripting
- Transversal Directory
- Authentication Bypass
- Error of logic : bypass security restrictions , access to Private Information
- Parameter manipulation of GET / POST requests / XML / SOAP
- Fuzzing
- Identity by manipulating session cookies theft
- Access interfaces / features hidden administration
- Upload functions of unsecured
- Permanent and Reflected Cross-Site Scripting (XSS)
- Phishing attack via RSS script
- Buffer overflows
- Known vulnerabilities (CVE, Exploit- DB, etc.).

The main countermeasures proposed by OWASP are implemented against the 10 main vulnerabilites of Web Applications.

The platform Accengage therefore has a high level of security and has been approved by major customer requirements.
The last audit was made in April 2017 by Lexfo (Report on request) and no vulnerability was identified during the audit phase in black box.

II.7 Access Control and Data Protection by Default Principle

II.7.1 Access to the Data servers

Accengage uses remote SSH secured access to servers, with IP filtering.
Database servers are placed in a private network unreachable from the outside.
Each relevant individual has individualized login and passwords and relevant access rights (Super Administrator, DataBase Administrator, Developer…). Approbation and revocation is determined by CTO and Super Admin (Least Privilege policy).
Passwords are comprised of minimum 8 characters (at least 1 letter, 1 number and 1 special character) and rotate every 3 months.
Detection of intrusion patterns are handled by Claranet. All accesses are logged and traced as well as all user actions. Accounts can be locked out in case of multiple access errors and trigger a lockout period.
The data for each customer and application are stored on separate databases with separate access.

Customer backend may connect to Accengage Backend using REST APIs (https protocol and Token request), or secured FTP / VPN (openSSH protocol).

II.7.2 Access to the application service

Access to the service is secured by management profiles. Each profile is connected with login and password and has certain rights giving access to different parts of service, and applications defined.
Accengage creates a client Administrator profile with certain rights, including the creation of new profiles. The administrator then creates the desired profile, and affects the available rights to these new profiles. Each child Customer credential inherits at maximum from the same access rights, preventing any errors in attribution.

Accengage has Admin profiles with access to all parts of the service and all applications (this profile is used for general maintenance and support service), as well as "Restricted Admin" profiles which have access to all parts of the service but for a limited number of applications (for project management and account management).
The Accengage employees have contractual commitments, are regularly trained and are made highly aware to security and confidentiality issues, as well as their responsibility and the consequences in case they do not follow the Security Policy for Information Systems.

Passwords must be comprised of minimum 8 characters and at least 1 uppercase letter and 1 number. All accesses are logged and traced as well as certain critical user actions. Accounts are locked out in case of 3 consecutive access errors and can only be reset by Accengage support or another Customer Local administrator.
All passwords are stored encrypted in SHA-2.
There is an automatic disconnection after 10 minutes of inactivity.

II.8 Organizational measures to secure user data

II.8.1 GDPR specific processes

Accengage has implemented certain measures which are specific for GDPR:

- Accengage has appointed a **Data Protection Officer** within the company, in the person of Nicolas Klain (nklain@accengage.com)
- Accengage signs **Data Processor Agreements** with its customers (and it has been the case since many years with its German Customers)
- Accengage maintains **Records of Processing Activities** (although it is an obligation for companies over 250 employees).

II.8.2 Incident Response Plan

Accengage offers a high level of security and monitoring through:

- Equipment redundancy
- Database replication
- 7/7 24/24 monitoring of Claranet.

In case of an incident (including Breach on personal data), the Incident Response Plan has 4 major objectives:

- Detect incidents, classify them and determine the right course of action
- Allow for regular service functioning as quickly as possible
- Minimize negative impact on business activities, respecting SLAs
- Capitalize on incident resolution knowledge.

There are successive cycles including:

- Detection and registering the incident (ticket creation)
- Diagnose for classification (network, security, hardware, application, storage, system, external…)
- Escalation based on nature of incident
- Client information based on level of incident criticality
- Resolution
- Ticket closing, documentation of incident and procedure updating if needed.

The categorization (automated or manual) of a ticket into a security incident immediately triggers several actions:

- real-time warning of the members of the comity to monitor operationally the Information Security Policy (ISP)
- identification of the involved assets and evaluation of the impacts
- triggering of a crisis cell (depending of level of impact)
- urgent communication to the relevant contacts at Accengage and Claranet who join the Crisis Cell.

- urgent communication to the identified contacts by the Customers which are impacted by the incident, who then join the Crisis Cell (depending of level of impact). Specifically, in the event of a **Breach on User Personal Data**, the Customer will be notified and the extent of the Breach will be communicated so that the Data Controller can notify the Regulation bodies.
- urgency measures implementation (if relevant)
- Security investigations
- Incident resolution
- Proof collection.
- Incident closing.

Once the incident is closed, information and proof are analysed in order to write an incident report, which will be sent to the Accengage managers. This document describes:

- history of the incident
- level of severity and impact on the platform
- root cause
- the circumventing or correction actions which led to incident resolution.
- the improvement actions, potentially identified by Accengage and Claranet.

The review of security incidents is done during the committees for operational piloting of Information Security Policy (ISP). Correcting or preventing actions can be executed relative to these.

II.8.3 Awareness Program & Information Security Policies

First of all, all of Accengage Staff has a Security awareness clause in their work contract covering: privacy, security, professional secret and confidentiality.

Instructions, presenting the great principles of the ISP (Information Security Policy), the security and restrictions to the usage of Accengage Information Systems (IS), the rights and obligations of users, the controls carried out by the IT teams and the consequences in case these rules are not followed, are transmitted to each user upon arrival.
During these information sessions regarding security, users are made aware, by their managers and the Information Systems Security Manager, of their responsibility, of the good security practices of Information Systems (IS) usage, and are also warned of disciplinary (following rules contained in the Personnel Status) or penal consequences in case of misuse or illegal use of the Information Systems (IS).
These rules are presented to each new agent whether hired on temporary, definitive or external basis, and are given before access to information and service is granted.
Regular actions of information are carried out by managers and by the IS Security Officer, by means of communication letters, news via the Internal channels (intranet, groups...) or specific events (seminars, themed breakfasts etc.).
After each yearly audit, the guide for good practices regarding Security is updated by the IS Security Officer and shared with the developers and employees.

The Information Security Policies are reviewed and maintained by the Organisation Committee for Information Security (OCIS). This OCIS is comprised of the CTO, the Information Systems Security Manager, an employee of the Audit & Administrative department, and of representatives for each entity which are involved in the ISP.
The OCIS is in charge of defining, approving, communicating and modifying the ISP. The OCIS produces and validates a communication plan for the ISP and its rules.
The OCIS is in charge of handling exceptions (events not taken care of in the ISP) having an impact on Accengage IS security.
The OCIS plans and implements a control of the policies on a yearly basis. This control is either done via internal audits or delegated to third party specialized entities, in charge of verifying the application of the rules set in the ISP.

II.8.4 Desktop / Laptop / Server security

Accengage corporate hardware benefits from a high level of security:

- Strong passwords are enforced
- Market-recognized Antivirus and firewalls are installed and updated on all devices
- Administrator control over machines and activities. Permission must be granted to install software.

II.8.5 Equipment disposal

Corporate hardware equipment is internally recycled. If no other option, equipment is destroyed by a specialized third party.

When the server hardware is at end of life, the information in this hardware is destroyed in accordance with deprovisioning process. This process involves the physical destruction of removable media and secured erase of the data on the hard drives. To do this, our host Claranet uses Darik's Boot and Nuke software algorithm with DOD-short (3-pass secure erase).
In the particular case of a formal disposal, hard drives are physically crushed by a hard drives mechanical destructive.