Version March 14, 2023

Technical and Operational Measures (including Security Requirements)

Organizational Safeguards

- Vendor must sign a non-disclosure agreement, which must then be co-signed by an IPSOS executive, prior to be granted access to Ipsos data and/or environment
- Vendor has appointed an employee who has data protection and information security responsibilities set out as part of their duties.
- Physical access to the building is limited by various access control mechanisms (for instance key cards) and in most cases entrances to Vendor's offices are staffed by receptionists/security staff.
- Vendor employees are instructed on data protection and information security matters upon commencing employment with Vendor and are subject to confidentiality obligations.
- Employees are not permitted to record Personal Data on a storage medium (e.g. disk) to enable them to re-access the information in premises that are not controlled by Vendor.
- In the event that Personal Data is held in hard copy format, any employees dealing with such Personal Data operate a clear desk policy, so that no Personal Data is left unattended in their absence. Personal Data in hard copy form is stored securely to prevent any unauthorized access.
- A business continuity plan shall be put in place and tested yearly

Information Security Risk Management

- Vendor must periodically assess risk within Information Technology specifically toward assets associated/involved in the services/products delivered to Ipsos. The implemented risk management framework should be in agreement with the requirements of the ISO 27001 & ISO 27002 or ISO 31000.

Information Security Policy

- Vendor must document their Information Security Policies and follow Information Security programs that are based on at least one of the following frameworks:
  - ISO 27001 & ISO 27002 standards
  - NIST 800 Special Security Publications.

- Vendor must map their security program to one of the above security frameworks showing no gaps in their information security program.

Information Security framework

- Vendor must define, document, and assign ownership to oversee development, adoption, enforcement and compliance with Information Security requirements, policies, standards, and procedures.
- Vendor must ensure the assigned role must be of a sufficiently high-level classification in the organization that can be allowed to execute the responsibilities in an effective and independent manner.
- To avoid conflicts of interest, Vendor must ensure this role will not have direct responsibility for information processing and technology operations.

Asset Management

- Vendor must design, document, implement and maintain an asset management process – having in scope the Vendor assets -, having the possibility to map the dependency between Vendor assets and Ipsos assets - including informational assets.
- Vendor must assign designated individual that is responsible for all Vendor Assets that access Ipsos assets and data.
- Vendor must document and implement rules for the acceptable use of assets of third parties, including without limitation, Ipsos assets and data.
- Rules of acceptable use must require that third party assets are not to be used for activities which have been identified as unacceptable conduct.
- Rules of acceptable use must require that third party assets are to be used in a professional, lawful and ethical manner.
- If Vendor connects to or use Ipsos asset(s) (including servers, workstations, infrastructure, internet gateway or network) must abide by all applicable Ipsos terms of use, policies, standards, and procedures.
- Vendor is required to safeguard and use Ipsos assets wisely and will use good judgment and discretion when using Ipsos assets including Ipsos systems, computers, telephones, internet access, email, voice mail, copiers, fax machines, vehicles or other property.

- Vendor must never connect non-Ipsos owned assets to Vendor’s network without direct written approval from Ipsos.
- Ipsos must review and approve all requests from any company to connect non-Ipsos owned assets to the Ipsos network.
- Assets that connect to Ipsos network must abide by Ipsos Security Policies, Standards, Operating practices and controls, including, but not limited to configuration, hardening, patching, access control and virus protection processes.

Human Resources Security

Vendor must:

- Ensure all Vendor employees, Vendors, and subprocessors who access Ipsos assets are screened prior to employment. Screening must include criminal, financial, employment background screening processes, while not conflicting with the applicable legislation.
- Have processes in place to periodically screen personnel during employment for anyone who accesses Regulated, Confidential, or Personal information.
- Ensure an Information Security awareness campaign is provided to everyone who has access to Ipsos assets. Campaign must educate personnel of their responsibility to secure Ipsos assets.
- Ensure all user IDs, tokens or physical-access badges are assigned to a unique Vendor employee or Vendor subprocessor.
- Ensure all user/system/service/administrator accounts and passwords are never shared.
- Immediately notify Ipsos in writing if a Vendor employee or subprocessor is not working on the Ipsos account or ID permission must be changed on a Ipsos managed assets and data. Notices must include name, user ID name of any accounts the person had access to or knows the password.

Physical and Environmental Security

Vendor must implement all the necessary information security controls in order to assure that all Vendor assets involved in the services provided to Ipsos as well as any Ipsos assets existing in Vendor custody are protected from:

- Natural disasters,
- Theft, physical intrusion, unlawful and unauthorized physical access,
- Ventilation, Heat or Cooling problems, power failures or outages.

<u>Operations Management</u>

Network Security**:** Vendor must deploy Data Loss Prevention (DLP) and or intrusion monitoring services at perimeter points where Ipsos regulated, confidential or Personal Data is used.
Vendor must ensure all unnecessary services, ports, and network traffic are disabled on all IT systems that access Ipsos assets.

System Security**:**
Vendor must have a process for applying and managing security updates, patches, fixes upgrades, (collectively referred to as "Patches") on all Vendor IT systems.

- Vendor must ensure patches that provide security fixes or security updates are tested and deployed within 20-days from the date of release, for all Vendor IT systems that access Ipsos Confidential, Personal, or Regulated Information.
- Otherwise, Vendor must ensure patches are deployed within 30-days from the date of release.
- All exceptions are to be documented while stating the reason for not deploying the mentioned patches.

Vendor must ensure Malware, Virus, Trojan and Spyware protection programs are deployed on all IT systems that access Ipsos assets and data; the mentioned must have the latest and up-to-date manufacture's signatures, definition files, software and patches.
Vendor must ensure all unused or unnecessary software, applications, services, sample/default files and folders are disabled on all IT systems that access Ipsos assets and data.

Operation Security - Vendor must**:**

- Ensure that any changes to IT systems that are performing work on or for Ipsos do not have any negative security implications.
- Follow documented change management practices and procedures
- Not move or transfer Regulated, Personal or Confidential information to any non-production environment or insecure location.

Disaster recovery

- Vendor has implemented appropriate disaster recovery measures to ensure that the Personal Data it processes can be re-instated in the event of loss or destruction of that data.
- The disaster recovery plan which will implement the disaster recovery measures will define RTO (Recovery Time Objectives) and RPO (Recovery Point Objectives). The RPO and RTO will be communicated inside of the DR Plan to Ipsos within 20 business days of the contract signature.
- Vendor periodically reviews these technical safeguards to ensure their continued suitability in light of the data it processes and technological advances.

Data management

Data Security

Vendor must:

- Use strong encryption key management practices to ensure the availability of encrypted authoritative information
- Encrypt all Ipsos data assets in transmission between Vendor and Ipsos as well as between Vendor and all other third parties when transmitted data is Ipsos data.
- Encrypt Ipsos confidential information at all times; encryption must meet a minimal standard of AES-256-bit encryption.
- In the case that a public/private encryption tool is used, Vendor must take every step to protect the private key.
- When encrypting Ipsos data do not send passwords/passphrases via e-mail or via voicemail
- If a password/passphrase is used in the encryption of the document, communicate the password/passphrase for the encrypted document out of band:
- Face to face
- Live on the telephone

Transferring of Data

Acceptable Methods of Data Transfer:

- Secure File Transfer Protocol (SFTP): SFTP is an encrypted version of FTP that uses SSH to transfer data securely between clients and servers, ensuring the confidentiality and integrity of the data.

- File Transfer Protocol Secure (FTPS): FTPS is an extension of FTP that adds support for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cryptographic protocols to encrypt data during transmission.

- Hypertext Transfer Protocol Secure (HTTPS): HTTPS is an encrypted version of HTTP that uses SSL/TLS to secure communication between web servers and clients.

- Virtual Private Network (VPN): A VPN creates a secure, encrypted tunnel between devices, enabling secure data transfer over public networks.

- Encrypted Email: Secure email solutions like PGP (Pretty Good Privacy) or S/MIME (Secure/Multipurpose Internet Mail Extensions) provide end-to-end encryption, ensuring the confidentiality of email communication.

- Encrypted Cloud Storage: Services like Google Drive, Dropbox, or Microsoft OneDrive provide secure data transfer options by encrypting data at rest and during transit, with options for additional layers of security like two-factor authentication.

- Managed File Transfer (MFT): MFT solutions offer centralized, secure, and auditable file transfers by using encryption, access controls, and monitoring to protect data during transit and at rest.

- Remote Desktop Protocol (RDP) over SSL/TLS: Using RDP with SSL/TLS encryption ensures a secure connection between remote clients and servers, allowing for the safe transfer of data between the devices.

- Secure APIs and Web Services: RESTful APIs and web services using HTTPS, OAuth 2.0, and API keys can provide secure data transfer between clients and servers. These security measures ensure that only authorized clients can access and manipulate data.

- Amazon Web Services (AWS) S3 Buckets: AWS S3 is a scalable storage solution that can be used to securely store and transfer data. By default, S3 buckets are private, and data can be transferred securely using SSL encryption. Additional security measures, such as Identity and Access Management (IAM) policies, bucket policies, and encryption options, can be implemented to further protect the data.

Unacceptable Methods of Data Transfer:

- FTP (File Transfer Protocol)
- E-mail
- Third Party file transfer Websites like www.yousendit.com , www.sendbigfiles.com and www.mailbigfile.com

Handling of Data
Only those staff from Vendor assigned to the specific Ipsos project for which the sample is intended may handle the client data provided by Ipsos.

- Vendor must ask Ipsos's permission to transfer Ipsos provided client sample onto any other vendors or sub-Vendors.
- Vendor's sub-Vendors must follow the same procedures for the transferring and handling of Ipsos provided client sample as outlined in this document.

Storage of Data

- Vendor to store Ipsos provided client sample on a server that is physically secured and is only accessed by authorized staff.
- Vendor to store Ipsos provided client sample on a server that is protected behind a firewall and that is properly patched with the latest OS and Security patches.
- Vendor to omit the directory in which Ipsos provided client sample is stored. This is to avoid Ipsos provided client sample from being inadvertently retained on Vendor's backup tapes for an extended period of time.

OR

- Vendor can backup Ipsos provided client sample to backup tapes as long as they are only used for disaster recovery and are not retained. Tape must be overwritten after a set amount of time.

Data destruction process
Vendor must assure that:

- Working storage media will either be wiped, shredded, stored or degaussed;
- Non-working storage media will be shredded, stored degaussed as follows:

Degaussing
For those regions with a degaussing unit, all hard drives and magnetic media such as tapes will be degaussed before disposal.

Hard Disk and Media Storage

- Functioning or non-function hard disks or electronic media such as tapes awaiting destruction by means of shredding, degaussing or wiping must be stored in a secured location with access to the room/safe/filing cabinet only given to those staff who need access to the media.
- A list of who has access to the media will be maintained
- A list inventorying all hard disks and electronic media such as tapes will be maintained and updated as hard disks and electronic media are added/destroyed. The inventory will list the serial number for hard disk and tape labels/names for tapes. The list will also list the status and state of the hard disk.
- This inventory will be reviewed twice a year to check for any lost or stolen hard disks and electronic media.

Media Destruction Standards

- Vendor must consistently demonstrate that they are in control of our information assets (i.e.: hard drive/tapes) up to and including their destruction.
- Confirmation of destruction of our media must be given within next business day of its disposal.
- Hard Drives will be disintegrated to a particle size no greater than ¼ inch or 0.635 cm.
- CD's, DVD's, Backup tapes, audio cassettes, and video cassettes are shredded to ½ inch or 1.27 cm.
- Paper documents will be shredded cross cut on site.

Hard Disk Wipe Standards

- All hard disks ready for destruction or disposal must be wiped using the DBAN utility.
- Wipe Method of US DOD
- 7 passes
- Enable Verification

Data Breach Procedure

A breach of information is any incident that involves the actual or suspected breach of the confidentiality, integrity or availability of an Ipsos information asset. In the case of Vendor, it is referring to the Ipsos provided client sample.

Examples are:

- *Theft or loss of a laptop, PC, USB Key, small computing device or any other computing/storage device that contains any Ipsos provided client sample.*
- *Suspected or otherwise confirmed unauthorized access (hack) into Vendor's network/hosts that holds Ipsos provided client sample.*
- *Successful virus/malware attack on a system that holds Ipsos provided client sample.*

In the event that any Ipsos provided client sample is breached to the public by Vendor, the following incidence response will be carried out by Vendor:

- Vendor shall notify their contact at Ipsos of the breach.
- Vendor will immediately launch an investigation into the data breach.
- Vendor will co-operate with Ipsos in the investigation and will share all relevant system logs and evidence with Ipsos immediately.
- The investigation will examine the root cause analysis in order to determine causes and recommendations for improving Information Security; to prevent future incidences.
- A risk assessment and recommended counter measures will be included in the final report.

Access Management

Vendor must:

- Ensure controls restrict other Vendor customers from accessing Ipsos assets, unless this has been specifically approved in writing by Ipsos
- Use authentication and authorization technologies for service, user and administrator level accounts.
- Not allow Vendor employees or subprocessors direct root access to any systems or access to the administrator user account of any system used in the services provided to Ipsos
- Ensure IT administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administrator tasks must always be performed using non-administrator user accounts.
- Ensure password policies and standards exist on IT systems that access Ipsos assets
- Ensure systems that access confidential, personal or regulated information require the following password construction requirements at all times:

i. Minimum length of 8 characters
ii. Complexity must contain at least three of the following four characters (Number, Uppercase Letter, Lowercase letter, Printable special character)
iii. When changing or rotating an account password, the reuse of any of the prior 6 passwords is not allowed
iv. Account password expiration (the requirement to change and existing account password), must occur at - or less than 90 days.
v. Service accounts must be changed at - or less than 90 days.
vi. Failed login attempts, when exceeding 3 consecutive attempts, must lock the account.
vii. Screen saver locks must be enabled to lock access after 30 minutes of user inactivity.

Vendor must ensure systems that access Ipsos assets &/or Ipsos network meet the following additional requirements at all times:

i. Authentication credentials must be encrypted when stored or transmitted at all times
ii. Passwords for user-level accounts cannot be shared between multiple individuals
iii. Vendor must change passwords immediately whenever it is believed that an account may have been compromised.
iv. Passwords must not be communicated via email messages or other forms of electronic communications, other than one-time use passwords.
v. Passwords for individual user accounts must never be given to or shared with
vi. someone other than the account owner
vii. A user's identity must be verified before their password is reset and email or voicemail notification must be sent to notify the user that their password was reset.
viii. First time passwords for new user accounts must be set to unique values that follow the requirements set forth in this policy and must not be generic, easily guessed passwords.
ix. User accounts must be configured to force a change of their password upon first use of a new account or after a password is reset.
x. All manufacturer passwords must be changed from their default values (including when the default value is NULL) and must meet the requirements set forth in this policy. Manufacturer passwords include, but are not limited to, SNMP community strings, system-level administrator account passwords.
xi. Temporary account passwords, wireless encryption keys, and other default authentication settings.

xii. Password fields must display only masked characters as the user types in their password, where technically feasible.
xiii. Hardcode plain-text passwords must not be used in production environments.
xiv. Production account passwords must not be used in non-production environments.
xv. If a system-level administrator account (e.g. Windows local administrator or UNIX/Linux root) is used to perform privileged management of a device, that password must be changed following completion of that management task.
xvi. If an account has machine-set complex password of 20 characters or more that is never accessed or known by a person, that passwords does not need to be changed during its lifetime, unless the account or its associated system has been suspected of compromise.
xvii. System-level account passwords must be unique on each device.
xviii. All systems must prompt users to re-authenticate when users attempt to elevate their privileges to higher security levels. *Examples include use of sudo or su on UNIX/LINUX systems or "run as" for Microsoft Windows based systems*.

- Vendor must ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.
- Vendor must ensure procedures exist for provisioning privileged accounts.
- Vendor must periodically review the necessity of privileged access accounts
- If Vendor requires remote access to Ipsos assets, Vendor must always use a Ipsos approved method to remotely connect to any Ipsos asset.

Information Technology Acquisition, Development and Maintenance

Vendor must:

- Ensure infrastructure, network and application vulnerability assessments are periodically conducted and follow industry acceptable vulnerability management practices
- Ensure industry acceptable application development security standards are followed so that IT systems and applications are tested and secured in every step of the application and system development life cycle.
- Ensure software and application source code are validated and tested against vulnerabilities and weaknesses before deploying to production.

Information Security Incident Management

Vendor must:

- Ensure access and activity audit and logging procedures, including access attempts and privileged access, exist.
- Ensure logging includes all facility, application, server, network device and IDS/IPS logs are centrally managed and maintained for no less than 12 months.
- Ensure security incident response planning and notification procedures exist to monitor, react, notify and investigate any incident related to Ipsos assets.
- Immediately notify Ipsos if Vendor identifies a breach in any controls that impacts the service provided to Ipsos, a Ipsos asset or data related to a Ipsos asset.
- Note: Once Vendor discovers or are notified of a security breach, Vendor must investigate, fix, restore and conduct a root cause analysis.
- Provide Ipsos with results and frequent status update of any investigation related to Ipsos.
- Vendor must permanently inform Ipsos Global Information Security staff on the investigation outcome.

Outsourcing

Where a service is outsourced by Vendor, the process must be managed by the relevant Vendor staff and a contract must be in place that covers all Ipsos information security requirements.

Filing for a policy Exception Request

Information security policy exception requests must be justified by Vendor and approved in writing by the Global Information Security Staff.