Third Party Information Security Management

Standards Document

Version 1

Produced:
March 10, 2023

Edited:
April 19th, 2023

Written by:

Dawn Kosakewich - Technical Marketing Specialist
Paula Amador - Chief Product Officer

Approved by:

Paula Amador - Chief Product Officer

1. Purpose

Expresia recognizes the importance of maintaining the confidentiality, integrity, and availability of its information assets, including those managed by third-party vendors. As such, it is the policy of Expresia to establish and maintain a Third-Party Information Security Management Program that outlines our expectations and requirements for third-party vendors with whom we share our information assets.

This policy applies to all individuals who engage with a third-party on behalf of Expresia, including but not limited to employees, contractors, and agents. The policy requires all third-party vendors to comply with the security and privacy requirements outlined in our contractual agreements and to adhere to the standards and guidelines set forth in this document. Special consideration in the policy is given to information sub processors as detailed in this document.

The Third-Party Information Security Management Program is designed to ensure that all third-party vendors comply with applicable laws, regulations, and industry best practices for information security and privacy. This includes conducting due diligence on third-party vendors before engaging in business with them, as well as ongoing monitoring and assessment of their security practices.

The program requires that all third-party vendors undergo a thorough assessment of their security controls and practices to ensure that they meet our minimum requirements for information security and privacy. Expresia will use a risk-based approach to determine the level of assessment required for each third-party vendor, based on the sensitivity and criticality of the information assets being shared.

This program also requires that third-party vendors undergo regular audits and assessments to ensure ongoing compliance with our information security and privacy requirements. Any identified deficiencies or vulnerabilities will be addressed through corrective actions and/or risk mitigation strategies.

Expresia is committed to working closely with our third-party vendors to ensure the security and privacy of our information assets. We expect all third-party vendors to demonstrate a similar commitment to information security and privacy and to work collaboratively with us to maintain a secure and resilient information environment.

2. Policy

This program is designed to ensure that all third-party products and services utilized by Expresia meet our security and privacy requirements. To achieve this goal, the program employs a risk-based approach that includes a thorough assessment of third-party security controls, ongoing monitoring, and contractual provisions that hold third-party providers accountable for maintaining the security of Expresia's information assets. The following strategies outline the steps that will be taken to assess and manage the security risks associated with third-party relationships.

2.1. Assessment

- Every third-party granted access to Expresia Information Resources must sign the Backbone Digital Third-Party Non-Disclosure Agreement.
- All third-party relationships that handle Expresia customer information must be evaluated for inherent information security risk prior to any interaction with Expresia's Information Resources.
- All third-party relationships must be re-evaluated for inherent information security risk biennially and any time there is a material change in how Expresia utilizes the third-party product or service.
- Third-party relationships with significant inherent risk must be evaluated for residual risk using questionnaires, publicly available information, and/or technical tools. Residual information security risk assessments must account for administrative, physical, and technical controls.
- Third-party relationships that do not meet established residual information security risk thresholds:
    - Must be evaluated for termination,
    - Must be formally approved by the Executive Committee, and/or
    - Changed in a manner that reduces inherent and/or residual information security risk to meet Expresia's established policy.
- Third-party relationships concerning industry and/or regulatory requirements (i.e. PCI-DSS, HIPAA, GDPR, SOC II, local data protection regulations in countries where Backbone Digital operates, etc.) must be reviewed on no less frequent than an annual basis.

2.2. Management

- Third-party agreements and contracts must be evaluated in a case by case basis by the Expresia technical team to determine if they should include information pertaining to
    - Information the vendor should have access to,
    - How information is to be protected by the third-party,
    - How information is to be transferred between Expresia and the third-party,
    - Acceptable methods for the return, destruction or disposal of Expresia information in the third-party's possession at the end of the relationship/contract,
    - Minimum information security requirements,
    - Information security incident response and notification requirements,
    - Right for Expresia to audit third-party information security protections and controls.
- If the third-party subcontracts part of the information and communication technology service provided to Expresia, the third-party is required to ensure appropriate information security practices are followed throughout the supply chain.
- Work outside of defined parameters in the contract must be approved in writing by the designated Backbone Digital or Expresia point of contact.
- Third-party performance will be reviewed biennially to ensure compliance with agreed upon contracts and/or service level agreements (SLAs). In the event of non-compliance

with contracts or SLAs regular meetings will be conducted until performance requirements are met.

- Any other Expresia information acquired by the third-party during the contract cannot be used for the third-party's own purposes or divulged to others.
- Third-party personnel must report all security incidents directly to the designated Backbone Digital or Expresia point of contact.
- Expresia will provide a technical point of contact for the third-party. The point of contact will work with the third-party to ensure compliance with this policy.
- Third-parties must provide Expresia a list of key personnel working on the contract when requested.
- Upon departure of a third-party employee from a contract, for any reason, the third-party will ensure all sensitive information is collected and returned to Expresia or deleted.
- Upon termination of contract, third-parties must be reminded of confidentiality and non-disclosure requirements.
- Upon termination of contract or at the request of Expresia the third-party must surrender all access cards, equipment and supplies immediately.

3. Enforcement

Expresia takes the security of its information resources very seriously and expects all individuals who engage with third-party products and services to do the same. To that end, any violation of this policy will be treated with the utmost seriousness and may result in disciplinary action, up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties. Expresia reserves the right to pursue any and all legal remedies available to it in the event of a violation of this policy.

Expresia will monitor compliance with this policy and reserves the right to audit third-party information security protections and controls. Any identified violations will be addressed promptly and may result in termination of the third-party relationship.

All third-party agreements and contracts must include a provision that requires the third-party to comply with Expresia's Third-Party Information Management Policy. Failure to comply with this provision may result in ceasing business negotiations or termination of the contract, whichever applies.

It is the responsibility of all personnel to report any suspected violations of this policy to the Backbone Digital Chief Technology Officer or using support@backbone.digital. Expresia will investigate all reported violations and take appropriate action to address any violations found.

4. Subprocessors

Expresia relies on subprocessors to provide essential products and services that support our operations. While we cannot control the content of their contracts or SLAs, we still hold these subprocessors to high standards of information security.

To ensure that subprocessors meet our standards, Expresia will conduct due diligence before entering into any new contracts with subprocessors. This due diligence will include an evaluation of the subprocessor's information security practices, risk management procedures, and incident response capabilities.

Expresia will annually review our use of subprocessors to assess whether they continue to meet our information security standards, or when a change in SLAs, security practices or information security changes materialize for any given vendor.

We will also require subprocessors to notify us immediately of any data breaches or security incidents that may impact our information resources. In the event a data breach occurs and the subprocessor fails to disclose to its clients, Expresia will revise the relationship with the subprocessor in the same terms as described for other third parties in this document.

In the event that a subprocessor requires access to Expresia information resources, a technical assessment will be conducted to ensure data privacy and legal compliance with main regulatory dispositions in Backbone Digita’s countries of operation.

Expresia is committed to maintaining a secure information environment and will continue to work closely with our subprocessors to ensure that they meet our standards of information security.

The following list of third-party applications are used by Expresia.

https://www.expresia.com/legal/expresia-subprocessors/