Confidentiality : Unrestricted Circulation

Eyvo Security Policies and Controls v1.1

Executive Summary

This whitepaper outlines Eyvo’s comprehensive security and privacy framework that protects client data across our global infrastructure. It summarizes our policies, compliance commitments, and operational controls designed to ensure the confidentiality, integrity, and availability of client data.

At Eyvo, we recognize you are entrusting us with one of your most precious corporate commodities - your data.

We take that trust in us very seriously, and to reflect that, we have prepared a set of internal policies, procedures, and controls that allow us to deliver our services to you in a secure and predictable way.

What is IT Security?

At the most fundamental level, IT security is about protecting things that are of value to an organization. That generally includes people, property, and data-in other words, the organization's assets.

Security controls exist to reduce or mitigate the risk to those assets. They include any type of policy, procedure, technique, method, solution, plan, action, or device designed to help accomplish that goal. Recognizable examples include firewalls, surveillance systems, and antivirus software.

Define Control Objectives First...

Security controls are not chosen or implemented arbitrarily. They typically flow out of an organization's risk management process, which begins with defining the overall IT security strategy, then proceeds to defining the goals. This is followed by defining specific control objectives and statements about how the organization plans to manage risk effectively. For example, "Our controls provide reasonable assurance that physical and logical access to databases and data records is restricted to authorized users" is a control objective. "Our controls provide reasonable assurance that critical systems and infrastructure are available and fully functional as scheduled" is another example.

... Then Define The Security Controls

Once an organization defines its control objectives, it can assess the risk to individual assets and then choose the most appropriate security controls to implement. One of the most straightforward models for classifying controls is by type: physical, technical, or administrative, and by function: preventative, detective, and corrective.

This document doesn't delve into the intricate details of what we do and how we do it. For a more detailed analysis, please refer to our Cloud Security Alliance CAIQ Document, available for download

at the bottom of the Security and Compliance page on our website. For more details, please visit the CSA website at https://cloudsecurityalliance.org/.

In this document, we provide a snapshot overview of the lengths we go to ensure our infrastructure, hosted environments, operational environment, and web applications are as secure as possible.

At Eyvo, we have a set of security Policies and Controls to help us :

- Identify network security issues and other vulnerabilities
- Identify policy compliance failures
- Improve employee awareness of proper security practices
- Assess an organization's effectiveness in responding to an attack
- They can be classified under three different event types.

1 Before the event

Preventive controls are designed to prevent incidents from occurring, such as by locking out unauthorized individuals.

Eyvo maintains an active policy of conducting black box penetration testing (pen testing) against both its own internal network and its primary eBA web application. We conduct regular bi-weekly tests with external White-Hat (ethical) hackers and third parties to ensure that our systems are as secure as possible.

2 During the event

Detective controls are intended to identify and characterize an incident in progress and mitigate it as fast as possible, e.g., Physical controls by sounding the intruder alarm and alerting the security guards/police; Logical Controls using IDS in our Firewalls to prevent inbound attacks over the internet. We can confirm that Eyvo has never detected any intrusions of its infrastructure or applications.

3 After the event

Corrective controls are intended to limit the extent of any damage caused by the incident, for example, by restoring the organization to its normal working status as efficiently as possible.

According to the nature of the specific events, we deploy the best tool for the job - for example:

- Physical controls, e.g., use of privacy screens, opaque doors/windows, digital locks, 'two-person' access to sensitive controls, and employee-issued RFID tags for access to secure areas, e.g., Server Rooms;
- Procedural controls, e.g., incident response processes, management oversight, logging contractor visits, secure document and data destruction, ensuring security awareness through training, checking job references for new hires;

- Technical controls e.g. user authentication (login), user roles, logical access controls, antivirus software is employed on every workstation and server, central Cisco firewalls are the front end of our network plus local software firewalls are employed on all servers and workstations, extensive use of 2FA technology for access to all of Eyvo's critical infrastructure pieces including access to corporate email, Federated AD to control SSO for access to our programming source code and system design docs for the technical teams.
- Legal and regulatory or compliance controls, e.g., privacy laws, policies, and clauses.

A similar categorization distinguishes control involving people, technology, and operations/processes.

Breaking it down a little more, Eyvo focuses on controls that are documented in a set of policies and procedures - developed both internally and via external consultants - Eyvo maintains policies on a number of fronts, including:

- Information Security Policy
- Human Resources Policy (Hiring/Termination)
- Acceptable Use Policy
- Access Control Policy
- Computer Maintenance Policy
- Incident Response Policy
- Remote Access Policy
- Disaster Recovery Policy
- Business Continuity Plan
- 3rd Party Engagement Policy
- Eyvo Office Operations Policy
- Change Management Policy

Some examples of the items these policies cover would include,

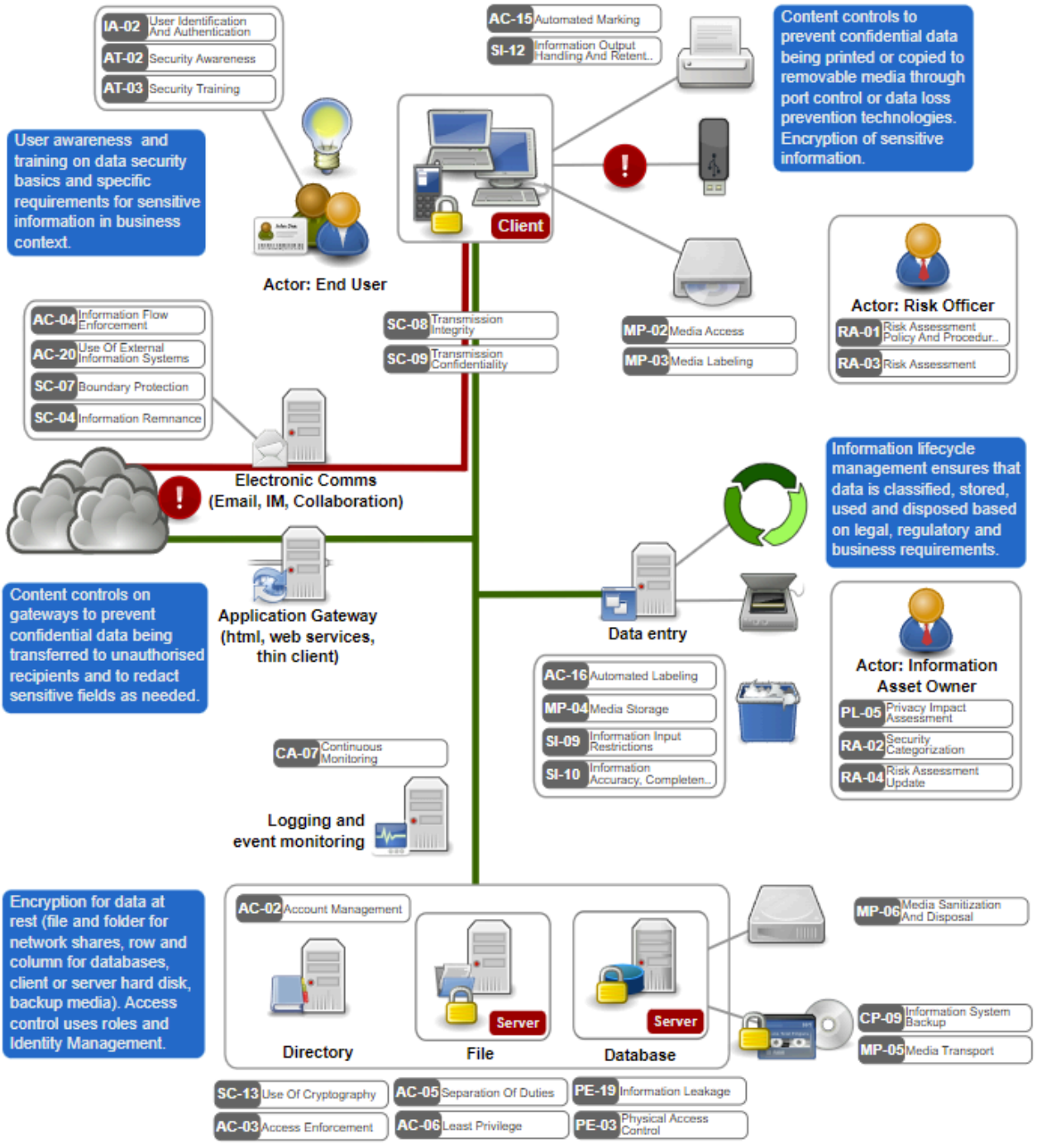
- Human Resources security - controls that are applied before, during, or after employment, e.g., Criminal background checks before employment, termination debriefing, returning key cards, disabling users' access controls, handing back equipment, disabling all logins and authentication methods
- Employee training - to bring awareness to all employees regularly, on the importance of social engineering and phishing attacks. All employee workstations disable links in emails and actively alert if any links need to be used
- Asset management, e.g., tagging all assets, identifying the location and the owner, Access controls, and managing user access via RFID-enabled keycards
- Cryptographic technology - Access to any of Eyvo's critical management software tools, e.g., Client Licence generation, is via the use of one-time keys generated via an app on a smartphone, e.g., Google Authenticator or Authy
- Physical security of the organization's sites and equipment via guards, cameras, and movement detection equipment

- Operational security, e.g., information is distributed and compartmentalized amongst all staff on a 'need to know' basis - Only key senior management have a total top-down view of operations that includes sales, marketing, infrastructure, technical development, security, and administration
- Access controls and managing user access via RFID-enabled keycards
- Secure communications, internal data transfer, and inbound network connections are only ever done using site-to-site private VPN; external connections (e.g., from Clients for ODBC SQL Server access) are only ever done using Static IPs from direct client sites where required.
- Security for suppliers and third parties, e.g., all 3rd party providers must have written contracts in place and undergo a security risk assessment, and any IT Infrastructure providers (e.g., Rackspace) must have SOC and NIST compliance, amongst others
- Incident management - any security incidents or suspected incidents are documented and logged
- Business continuity/disaster recovery for both ourselves and our clients (to the extent that it affects information security and availability). We maintain a 'hot' standby set of infrastructure by a secondary infrastructure provider - Rackspace is our Primary provider, and we run parallel hot standby sites in Microsoft Azure - e.g., if Eyvo's application or database servers were to be affected via a Ransomware attack, then we aim to be re-operational within 3 hours.
- Compliance - with internal requirements, such as our own policies, and with external requirements, such as laws, e.g., GDPR, SOX, etc
- Data Encryption: All client data in transit is protected via TLS 1.2+; data at rest is encrypted using AES-256.
- Change Management & Logging: mention centralized log collection, SIEM, or equivalent.
  Vulnerability Management: include patch management cadence (e.g., “critical patches within 24 hours”)
- Third-party Risk: We conduct periodic reviews of hosting vendors’ SOC reports.

Please refer to this web page for more information:

https://www.e-procurement.com/cloudinfrastructure

At Eyvo, one of the diagrams we use to help us understand these issues is shown below.



Here, you can see just some of the elements we need to be aware of and control as we provide our customers with the services we have been contracted to deliver.

Getting Ahead Of Incident Detection and Compliance Failures: Responsiveness

External penetration tests (pen tests) usually result in something being found. The reason for this is that at Eyvo, we have a rolling development program, where we constantly fine-tune our services and software. We want to ensure that we don't introduce any weaknesses related to our overall security in the process. Continuous pen testing is fundamental and intended to catch these issues.

We don't publish the results of our penetration testing, as doing so would invite any 'bad actor' to try their luck. However, typically, after any penetration test has been conducted, the vulnerabilities found are categorized into four main areas: Critical, High, Medium, and Low. To date, we have not seen any 'Critical' vulnerabilities reported after our penetration testing. However, if we were to, our procedures aim to mitigate them immediately upon discovery and repair/fix them where possible within 2 hours.

If we identify any internal compliance failures due to personnel not following our procedures, we retrain the staff member responsible and ensure that all our teams are aware of the failure to ensure compliance in the future.

EU–U.S. Data Privacy Framework (DPF)

Eyvo is a signatory of the EU-U.S. Data Privacy Framework (DPF), formerly known as Privacy Shield, and our entry can be seen here https://www.dataprivacyframework.gov/list. This means we comply with both US and European privacy rules through a resource mechanism overseen by the International Center for Dispute Resolution. In addition, we control and monitor,

- Types of personal data processed
- Purpose limitation and data minimization
- Client data segregation in multi-tenant environments
- Data subject rights handling (access, correction, deletion)
- Retention and deletion policy summary
- Provide a Statement about not selling personal data

For further information regarding this subject, please contact us at privacy@eyvo.com

Please refer to this web page for more information.

https://www.e-procurement.com/eyvo-legal/privacy-policy