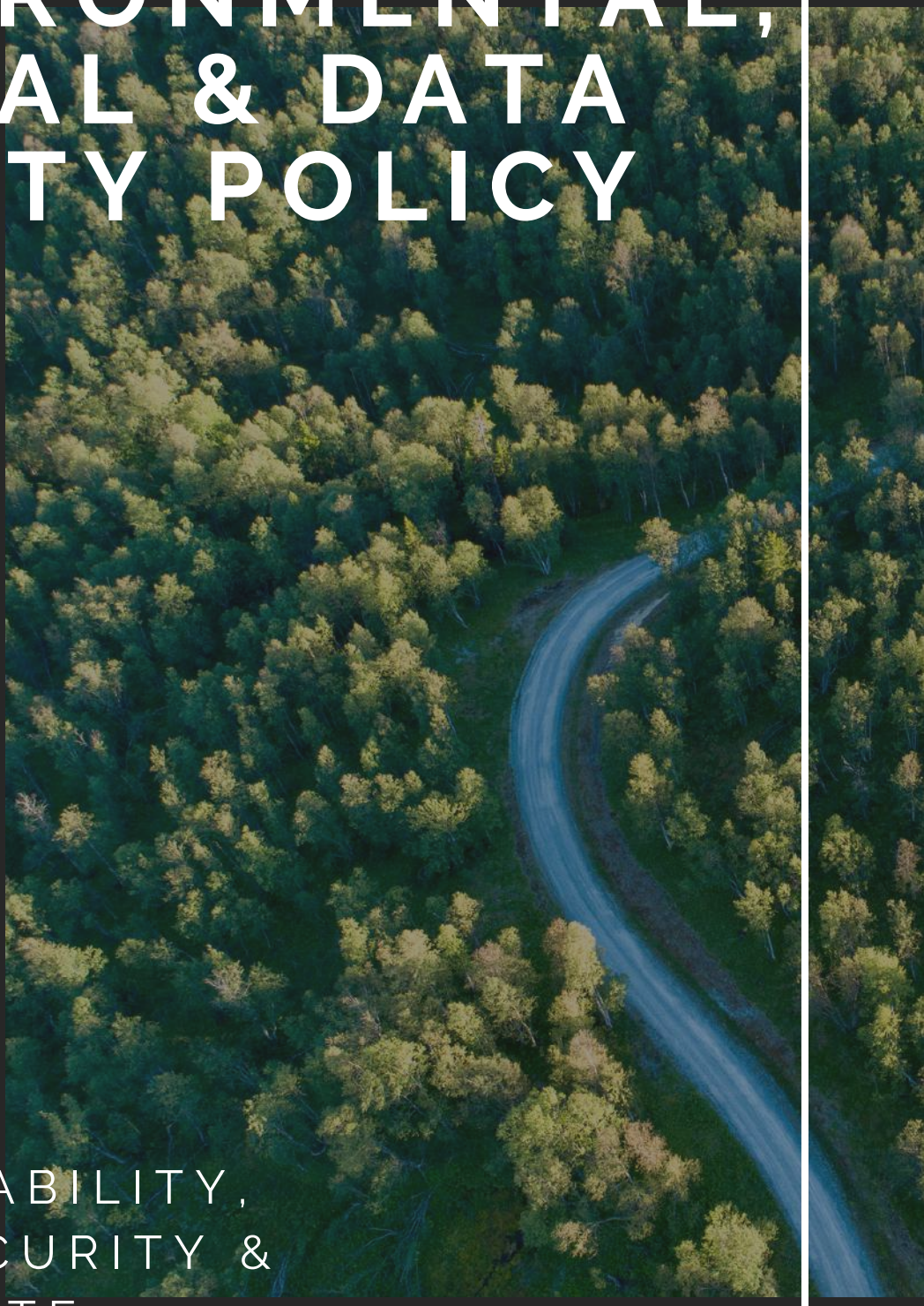
ClipSource

ENVIRONMENTAL, SOCIAL & DATA SAFETY POLICY



SUSTAINABILITY, DATA SECURITY & CORPORATE GOVERNANCE

FEBRUARY 2024

Table of Contents

Environmental Footprint

Clipsource provides digital products and services that streamline our customers' operations, processes and flows in several areas. As a consequence of our work, our customers' need to use physical media carriers such as video tapes, DVDs, portable hard drives and paper is reduced. In addition, our customers can achieve higher results with fewer resources. Overall, this leads to a significantly reduced environmental impact.

This environmental policy forms the basis for Clipsource's environmental work. This defines how Clipsource affects the environment, who is responsible within the organization and how the environmental policy is translated into goals and actions.

Responsibility

Clipsource carries out active environmental work in collaboration with customers, suppliers, employees and other stakeholders and strives to meet and exceed the requirements set. At a minimum, Clipsource must comply with applicable legal requirements with regard to environmental aspects.

Responsible for legal compliance and ultimately responsible for Clipsource's environmental work is the CEO.

The environmental policy must be communicated to all employees within the company and it is the responsibility of each manager to ensure that this happens within their own team. It is also the managers' responsibility to ensure that employees who are affected by specific goals, rules, routines or other information receive this information.

It is the responsibility of each employee to follow the rules and routines that the company has set up for its environmental work. Environmental management in the offices is handled by the administrative staff. The responsible purchaser is responsible for ensuring that environmental considerations are taken into account when purchasing for the company.

Environmental Aspects

In its operations, the company has identified the following areas as most important from an environmental point of view:

Recycling & E-waste disposal

The company's operations are for the most part of an office nature and in the daily work simpler forms of waste arise, for example paper, packaging, electronics, light bulbs and batteries. The company's policy is to minimize the amount of waste (e.g. by avoiding unnecessary printing and disposable packaging) and ensure that what is produced is recycled in an environmentally sound manner.

Clipsource aims at recycling electronics with the local e-waste recycling facilities that follow environmentally friendly practices. It is important for us to avoid disposing of electronic waste in regular trash as it may contain hazardous materials that can pose a threat to the environment and human health.

Purchase

When purchasing, it is primarily by choosing the environmentally best supplier or product that Clipsource can reduce its environmental impact. In all purchases and procurement of products and systems, the environment must be considered as a parameter. Consumables that are purchased must have one of the well-established environmental labels.

Energy

In our business, energy is consumed in the form of heat, hot water and electricity. Clipsource works to reduce energy consumption (e.g. by always turning off lighting and other electrical equipment when rooms are not in use or the office is unmanned). We must also have a room temperature that falls below 20 degrees in the winter.

Suppliers

Clipsource’s suppliers affect the environment through, for example, disposal of end-of-life or discarded equipment. Clipsource must, in addition to considering the environment when choosing suppliers, work to reduce the suppliers' environmental impact.

Chemicals

For the small amount of chemicals used, they must be approved by the internal manager and be the choice that works for the business with the least environmental impact.

Travel

When traveling on business, it is always considered whether any of the following measures are reasonable to implement: choice of more environmentally friendly means of transport, for example trains instead of flights; using alternatives to travel such as video conferences and choosing vehicles with a lower environmental impact. As far as possible, we will also share hotel rooms during trips.

Environmental Goals and Self-control

Carrying out active environmental work and reducing the company's environmental impact is an ongoing task with constant improvements. This environmental policy is updated annually and based on it, the identified environmental aspects are translated into environmental goals with action plans to achieve them.

Every year, a check must be carried out to see if the environmental goals are met. If this is not the case, an action plan must be drawn up. The CEO is responsible for this self-check.

Data Privacy & Security

Clipsource personnel are required to agree and adhere to all Clipsource's policies, rules and procedures, including applicable data protection policies.

Internal IT Operations

Passwords for both internal and external users are to be complex (a minimum 12 characters and to consist of a combination of upper- and lower-case letters, numbers, and special characters).

Sharing of passwords between users is not allowed and all logins with higher user privileges are to be logged and saved for 12 months.

In case of staff leaving their positions, encryption passwords are to be changed as well as all administrative passwords, codes for entry to the office and the user's account is to be deleted.

Any email correspondence regarding development is saved and the mailbox is stored for future reference and legal matters abiding by the rules and regulations of GDPR.
For new emails, the sender will get a reply referring to a new assigned contact at Clipsource.

Services provided to third parties are to be checked every day to ensure services. The services are written to be affected by a single code failure so one script failing will not affect the entire service thus ensuring resilience.

That said, all scripts are to be monitored and verified daily to ensure our services.

- Logins to the system are to be protected by valid SSL certificates and obsolete encryption methods are to be disabled on public systems. Physical access to systems is not possible since they reside on Amazon. There is however a policy document describing severe operations also for physical on prem servers should the need arise, see Peripheral equipment policy for more information.

- Access to applications or Clipsource systems is only allowed by relevant staff with valid usernames and passwords. Multi-factor authentication and VPNs are used for securing access and communications.
- The application environment is constantly monitored by predetermined security protocols and services where relevant staff is notified via email and/or Slack in case of any problems.
- Monitoring and IT operations are during business hours in Sweden.

Backups are to be encrypted and passwords and recovery manuals are only available to relevant staff. If possible, the backup encryption is not to be available to system administrators but the backup staff only to avoid restores of data to unauthorized locations. Any restore attempts are to be monitored and logged.

In cases of external consultants, minimum user rights are to be given and any created user account is to be automatically locked out after a given period (default is 48 hours). This is to ensure a minimized attack surface. Any external help is to be monitored and approved by staff at Clipsource.

Any external consultants are to sign and approve an NDA (Non-Disclosure Agreement) if deemed relevant and necessary by executive management.

Security and vulnerability scans are to be made regurarly at intervals of a maximum of 6 months. These tests may include different tools and methods such as using KALI Linux and Metasploit depending on the imagined scenario.

Development Processes and Operations

Any code written for Clipsource is the immaterial and intellectual property of Clipsource.

Clipsource is to be considered a multi-tenant system and treated as such. Any data leakage between users or customers is to be always avoided. Setups where customers have separated databases are to be totally isolated from other customers' data.

- Passwords are never to be stored in plain text, but are always encrypted in case of theft of the user database as well as to be non-visualised for our internal personnel.
- In case of data theft, the entry point is to be secured and all passwords are to be forcibly changed for all users.
- Source code versioning is managed in git, with origin hosting provided by GitHub. The codebase, valuable data and the applications are also to be backed up to a non disclosed offline location.
- In conjunction with GitHub, Clipsource also uses Jira to keep track of backlogs, upcoming and active sprints to ensure quality and planning. Within Jira there are built in verification processes and validations to ensure a compliant release and stability.

- Any code changes are well documented and traceable and any changes to code are to be verified and thoroughly tested on designated systems before implementation.

Failure & Backup

Should a new version fail for any reason, the backup plan is to be used to revert to the latest stable version as quickly as possible.

- Any new implementations are to be planned and if possible, users and customers are to be notified in advance of possible downtime due to upgrade.
- System downtimes are to be always avoided. However, major implementations that might result in a temporary downtime are to be planned and notified to customers at least one week in advance.
- The implementation process is done in three stages (DEV, TEST and finally PRODUCTION).
- Each of these environments are separated into different AWS accounts, with only the relevant access given. The production environment is the only environment having applications reachable from the open internet, whereas the other environments require VPN for both server access as well as reaching any application even for test or QA purposes. Access to each AWS account requires multi-factor authentication.
- Code into production can only be deployed by select users and is first run through a Development release, a Test release for quality checks before finally deployed into Production. Final testing of code deployed in Production is always carried out in connection with the deployment.

Fallback & Revision of Code

Fallback and reversion of code is built into the system and can be quickly used in case of unwanted or unexpected results. During a new implementation, a period of at least a week of higher monitoring and accessibility of staff is required to be notified of possible bugs or unforeseen errors. Prior to version releases, all aspects of security and usability are to be tested (SQL injections, directory traversals, changed user permissions, overload and DDoS attacks, brute force, and dictionary attacks and so on).

Internal IT Operations

This policy is reviewed at least yearly by management and any changes are communicated to relevant staff at staff meetings.

Hardware and other Property

Computers and any hardware are the property of Clipsource and should be used accordingly. Should an employee leave the company, any hardware is to be returned unless otherwise agreed upon.

All hardware and software are to be thoroughly inventoried and maintained. Any critical hardware (workstations, laptops, mobile phones) are to be locked away and stored safely overnight if left at the office. In case of theft, new hardware is easily acquired, and documents and software are available through daily backups. The most critical software and code is stored on Amazon providing our services. Use of removable media such as external hard drives or USB flash drives is not allowed.

General Guidelines

- As far as possible, biometric authentication methods should be enabled and used on any hardware that supports it. Passwords for both internal and external users are to be complex (a minimum 12 characters and to consist of a mix of upper- and lower-case letters, numbers, special characters) and they are to be unique to each user.
- Passwords are also to be changed every 45 days and are not allowed to be reused within one year.
- Sharing of passwords between users is not allowed and all logins with higher user privileges are to be logged and saved for 12 months.
- Passwords to shared services are to be controlled by using LastPass and two-factor authentication protection.
- Classes and courses in security are encouraged and necessary to maintain a high-quality service. There is no pre-approved or designated plan, but courses and classes deemed valuable for the employee and the company are approved.

Laptops and Workstations

Laptops are to have disc encryption software, BIOS passwords installed (where applicable) and complex passwords for unlocking.

- In case of laptops getting lost, the user is responsible for having relevant software installed to be able to wipe the laptop remotely to delete contacts, emails, and calendars. The employee is also to immediately report to management in case of loss.
- If possible, users should log in with only minimal rights to their own computers and have an extra administrative user available for software installations and so on. This is to minimize the risks of having unwanted software installed with too high user privileges.

- In terms of use of mobile equipment, there is an IT policy banning the use of company phones for personal use in cases such as installing unapproved software or surfing the Internet for non-work-related purposes.
- All workstations, laptops and mobile phones are to be used with caution and always be updated with relevant security patches and antivirus software.
- Work from home is to be conducted securely via pre-approved secured connections using multi-factor authentication and secured VPN connections.
- Installation of new software is to be done with extreme caution and only when deemed necessary.

Mobile Phone Policy

- Mobile phones are to be protected by PIN codes and screen locks and If available, also with biometrics such as fingerprints or face recognition.
- Any use of mobile phones, laptops or any hardware/software owned by Clipsource that violates Swedish law or business ethics will be a matter of legal action and render an immediate resignation.
- In case of mobile phones getting lost, the user is responsible for having relevant software installed to be able to wipe the phone remotely to delete contacts, emails and calendars. The employee is also to immediately report to management in case of loss.

Documents Policy

- Printing of documents should be avoided as much as possible.
- Sensitive documents are to be printed locally or the user is to make sure that unauthorized personnel can't view documents while printed on shared printers.
- Sensitive documents are not to be left publicly accessible at the office nor at home.
- Sharing of documents is to be done securely and, if possible, avoiding the use of public free services.
- All hardware that can be inventoried should be so. The inventory should be automatic and collect information about hardware, software, licenses, and security status.
- Software provided by Clipsource is the property of Clipsource and is not to be shared with third parties. Any licenses are the property of Clipsource and sharing of these may result in legal actions.
- Access to applications or Clipsource systems is only allowed by relevant staff with valid usernames, passwords, and multi-factor authentication.
- Printer access is provided within the Clipsource office network and secured as described in Server management, installation, and operations.

Managing Systemic Risks from Technology Disruptions

Clipsource uses Amazon for hosting of applications and therefore the physical data centers aspects are provided and maintained by Amazon.

In case of physical servers being needed, Clipsource does have policies on how they are to be managed and operated, see *Server management, installation, and operations* for more information.

For logical security, Clipsource relies on security solutions, backup and restore capabilities by Amazon.

Firewalls and settings abide by the OWASP rulesets including protection against:

- SQL Injection
- Cross Site Scripting (XSS)
- Bad bot and scraper protection
- Scanner and probe protection
- IP address whitelist/blacklist
- Known-attacker protection
- HTTP flood protection
- Cross-Site Request Forgery (CSRF)

The responsibilities for security and risk management are shared by the management, developers, and technical staff.

The incident management plan is highly dependent on the type of event. The escalation process is based on whether the entire system is affected or a limited number of users. The steps are to troubleshoot the cause by technicians, report to management who will have to decide the course of action depending on the incident. This can be a software malfunction, a hacking attack, an unexpected failure at Amazon or other kinds of disruptive events.

Whereas Clipsource is not ISO certified, we follow the steps as outlined in ISO 27035. ISO 27 035 outlines 5 phases of Information on Security and reaction to an incident, namely:

1) Planning and preparing,
2) Detection and reporting
3) Assessment and decision
4) Responses
5) Lessons learned

The IRT team (Incident Response Team) consists of developers, operational staff, and management.

Planning and Preparing

We have detailed and verified disaster recovery plans, business continuity plans and well documented channels of communications with external clients and partners.

Detection and Reporting

We rely on monitoring, alerting and manual checks of log files for any suspicious activity. All alerts are emailed and/or sent via Slack to resolver groups for assessment and mitigation.

Assessment and Decision

Phase three consists of determining the root cause and assessing priority and determining mitigation. In case of customer disruption. management will be informed and will have the responsibility to inform customers through previously agreed channels.

Responses

Responses vary on threat level and type of incident. There is no general plan for every possible scenario, but scenarios planned to include:

- Hacking attacks,
- Network disruption,
- Malicious code or unexpected code behavior, and
- Other infrastructural incidents.

Lessons Learned

After each incident, a report is gathered and examined to make our responses even more efficient in the future and, if possible, to prevent the same scenario from happening again.

In terms of hacking attacks, the software is maintained and checked regularly, and security news is monitored by both management and staff. Should a hacking attack occur, the course of action is decided by management regarding forensics and whether to revert to backups or whatever is deemed necessary at that time. The goal is to always provide secured and reliable services to our customers.

Should the management deem it necessary to alert and notify customers, this is done via email, phone, our website, help-center or by any other means required by the situation.

In terms of security for hardware and software at the local office, the policy is that workstations and other critical tools are locked away at night at the office and the entry to office premises is controlled by individual key cards and codes.

Peripheral Devices

There is also a detailed policy for operations and management of peripheral devices such as printers, scanners, mobile phones etc.

- Any device with a login is to be secured with a unique and complex password.
- Default passwords or even empty passwords are not allowed.
- This includes FTP services, management services for the device etc.
- The use of unencrypted protocols such as HTTP. FTP, SMTP are not allowed, and it is the responsibility of the system owner to make sure any device is properly secured using best practices.
- Switches and other central networking equipment is to be locked and secured and only accessible for select staff.
- Unused ports in switches are not enabled to minimize the risk of unauthorized users connecting to the office network.
- Monitoring of any new hosts is set up and alerting sent to relevant technical staff.
- Printing is to be configured using IPPS (Printing over SSL). Saving documents locally on printer drives is not recommended.
- Insecure protocols such as ports 21, 25, 80, 515, 631, 721-731, and 9100 are to be turned off and complex, administrative passwords to be used on any printer.
- Wi-Fi and Access Points are to be configured using WPA3 when supported and any access is secured with complex passwords.

At the office premises, there are also centrally administered fire alarms and burglar alarms.

Should a major event occur such as a natural disaster or terrorist attack, work is to be maintained by employees from home if possible. Clipsource does not have a plan for cold site offices, nor is this deemed necessary considering the nature of the services. The crucial part of the business is to provide services to customers over the cloud-based solution.

The risk management policy is an ongoing process and is reviewed and revised yearly or when new situations arise such as new security threats or political changes that may affect our business or clients.

Recruiting & Managing a Global, Diverse & Skilled Workforce

Core values

Trust

We know that you work with sensitive materials and information. We are proud that you trust us to be a gatekeeper for them. We also pride ourselves on being transparent with both positive and negative information. We are loyal to our customers and we never promise things that we can't deliver.

Trust internally	Trust externally
• Avoidance of micro-managing • Flexibility with remote working • Asking proactively when in the need of information • Acting in Clipsource's best interest when we use company resources	• Transparency - with both positive and negative information • Genuine care about customer security • Keeping promises and loyalty to customers

Smooth

The media industry is increasingly complex, and so is the daily work for media professionals, often with cumbersome and time-consuming workflows. Everything we do is designed to make your daily work run smoother. We are flexible and always available to respond quickly to our customers, because we know their conditions change fast.

Smoothness internally	Smoothness externally
• Respectful of differences • Solving of problems together without hierarchy • Friendly attitude & tone of voice	• Easy to use platform at all levels • Flexibility - because our customers' businesses change fast • Fast response to customers

Expertise

As a SaaS company that exclusively serves the media and entertainment industry, we take pride in being true experts in what we do.

This means listening more than we talk so we can develop a product that solves our customer's most pressing problems. And we always strive to exceed our customer's expectations.

Expertise internally	Expertise externally
• Employing & promoting great people • Proactive learning environment both individually & collectively • Documenting all work and processes	• Deeply understanding customer needs • Listening more than talking • Developing solutions that solve real problems • Constantly striving to exceed customer expectations

Inclusion & Equality

Clipsource has a commitment to diversity, equity, and inclusion, with efforts to promote a workplace where employees from all backgrounds and identities feel valued and respected as well as treating all employees fairly and equitably, regardless of factors like gender, race, ethnicity, sexual orientation, or disability status. Creating an inclusive and equitable workplace not only promotes a positive company culture but also drives innovation, productivity, and profitability.

By valuing diversity and ensuring that all employees have equal opportunities to succeed, Clipsource can attract and retain top talent, improve employee morale, and foster a sense of belonging among its staff.

Diversity in the Team

Gender Diversity

Our Stockholm team has a balanced gender ratio, with 45% of employees being women. This means that both men and women have an almost equal representation in the team, which leads to a more inclusive work environment where women feel heard and respected.

Ethnic & Cultural Diversity

Our team in Stockholm consists of individuals from different countries and ethnicities. This diversity in cultural backgrounds can bring a wide range of perspectives and ideas to the team, leading to more creative and innovative solutions.

Age Diversity

Our team has a wide age range, with employees ranging from 25 to 59 years old. This diversity in age can bring different perspectives and experiences to the table, which can be beneficial in problem-solving and decision-making.

Accessibility

Our office in Stockholm is designed to be accessible to everyone, including people with disabilities. This means that the workplace is designed with ramps, elevators, and other accessibility features, ensuring that all employees can work comfortably and without barriers.

Educational & Professional Backgrounds

Our team members come from diverse educational and professional backgrounds, with 12 different areas of specialization represented which brings in an even richer array of ideas.

Language Diversity

Our team in Stockholm collectively speaks over 13 different languages, making communication in the workplace more inclusive and accessible.

LGBTQ+ Support

Our team in Stockholm proudly includes and celebrates members of the LGBTQ+, both within our team as well as the local community.

Working environment

Flat Organizational Structure

At Clipsource, we pride ourselves on cultivating a collaborative and supportive team culture that values open communication, feedback, and transparency. We believe that every team member has a unique perspective and contribution to make, regardless of their position, and we encourage all employees to speak their minds and share their ideas. Our managing team recognizes the importance of taking into account different perspectives when making decisions, and we strive to foster an environment where every voice is heard and valued. We believe that creating a culture of open communication and transparency not only strengthens our team dynamics but also leads to better decision-making and outcomes.

Work-life Balance

At Clipsource, we recognize the importance of work-life balance and strive to accommodate our employees' personal and family needs. We offer a flexible work schedule that allows our staff to complete their work hours at different times outside of the standard 9 to 5 business hours, as long as they fulfill their work responsibilities.

This arrangement allows our employees to manage their work and personal commitments more effectively, promoting greater satisfaction and well-being.

While we encourage our employees to work from our office, we understand that there may be times when working remotely is necessary or preferred. Therefore, we allow our employees to work from home as long as they adhere to our security protocols and use the necessary equipment to ensure the same level of protection as in the office.

This flexibility provides our employees with the freedom and autonomy to work in a way that suits their individual needs while maintaining the same level of productivity and collaboration. Overall, our flexible work arrangements demonstrate our commitment to supporting our employees' work-life balance and well-being, promoting a positive and productive work culture.

Mental Health & Reducing Risk of Burnouts

At Clipsource, we recognize that our employees are our most valuable asset, and we prioritize their mental health and well-being. We believe that creating a positive work environment starts with promoting a healthy work-life balance and providing the necessary support for employees to maintain their mental and emotional health. To mitigate the risk of burnout, we take proactive measures to promote a healthy work-life balance and support our staff's mental and emotional health.

For example, we encourage our employees to take regular breaks and prioritize self-care during the workday. Our weekly check-ins are one way we stay connected with our staff, providing a forum for open dialogue and feedback. Additionally, at least half-yearly, we have a team session where we revisit our core values and discuss how our team attitudes and behaviors are aligned with our core values.

Our managers are trained to identify any potential issues and provide appropriate resources and referrals to support their team members. We also offer mental health resources and support services, such as counseling and mental health days, to help our employees cope with stress and maintain their well-being. By prioritizing employee mental health and well-being, we strive to create a supportive and compassionate workplace culture that empowers our staff to thrive both personally and professionally.

Career Growth

Clipsource places a strong emphasis on providing opportunities for professional development and growth for its employees. The company offers regular training and workshops to help employees enhance their skills and stay up-to-date with the latest technologies and industry trends. Additionally, the company offers mentorship programs, pairing experienced employees with those who are new to the industry to help them build their knowledge and gain insights into their roles.

Clipsource also offers employees to take advantage of our quarterly one-on-one “growth talks” with their nearest manager around personal goals for development. Together with performance evaluations this opens for promotion opportunities based on individual contributions and achievements.

Clipsource values social and community engagement and offers a range of activities to promote team building and networking. For example, Clipsource organizes regular team building events, such as social gatherings or outdoor activities, to encourage collaboration and strengthen relationships among employees.

Employee Engagement rate

For the leaders at Clipsource, we have responsibilities to ensure that tasks are performed correctly and up to standard within our area of responsibility, as well as creating the right conditions for high employee engagement, work satisfaction and growth. Therefore we are committed to ensuring that we have structured ways of working to ensure clear goals, continuous progress and active learning.

One of the many ways we measure this sort of feedback is through a yearly Employee Engagement Rate, where 12 questions are asked to our employees and managers taken from Gallup's Q12 Employee Engagement Survey. Gallup's Q12 is a measure of employee engagement that helps businesses evaluate the emotional commitment and involvement of their employees towards their work. The Q12 questionnaire includes 12 key indicators that can impact employee engagement, such as feeling valued, having opportunities for growth, and receiving feedback. A high Q12 score indicates that employees are more likely to be productive, satisfied, and committed to their work, which can lead to better business outcomes.

In our case, as of 2023 Clipsource scored a **8.64 out of 10** on the Q12 engagement rate, which is a testament to their team's happiness and satisfaction with their work. This has also helped the managerial team pinpoint in which components of employee engagement we are lacking or behind, therefore taking action before any serious issues could possibly arise. The score could also indicate that Clipsource is taking steps to ensure that their employees are engaged and fulfilled.