



RepRisk AG
Zurich | Headquarters
Stampfenbachstrasse 42
8006 Zurich, Switzerland

Phone
+ 41 43 300 54 40

Email | Web
contact@reprisk.com
www.reprisk.com

Employee Handbook – Global Policies

Employee Handbook – Global Policies

Table of Contents

Introduction to the Handbook.....	3
Purpose	3
Employee Responsibility and Compliance	3
Amendments	4
Learning about RepRisk	5
Global Policies and Procedures.....	6
Quality Assurance	6
Data Protection and Confidentiality	8
IT, Information Security, and Data Management	9
Safety	14
Environmental Sustainability	15
Code of Conduct	17
Gifts and Entertainment	18
Key Company Processes	19
Training Policy	23
Media and Communications	24

Introduction to the Handbook

Last updated: [October 15, 2021](#)

Purpose

The Employee Handbook (further referred to as “the Handbook”) is a compilation of key RepRisk global and local policies and procedures. The Handbook is meant to provide a source for employees to learn about and be guided by the key RepRisk policies and procedures. The Handbook consists of two parts:

Employee Handbook – Global Policies

The RepRisk Way (Code of Ethics)

It is meant to be read by every new hire, and referred to, as needed, by all staff throughout their employment at RepRisk.

The Employee Handbook Local Policies have been compiled on a separate document.

Employee Responsibility and Compliance

The rules, policies, and procedures defined in this document are compulsory for all employees of RepRisk. Every employee must confirm that they have read and understood the Handbook and are bound by it. If you have questions or require clarification on any of the clauses, feel free to reach out to your line manager and/or the HR Team.

In case of a noncompliance with RepRisk’s policies, disciplinary actions may apply. These may range from a verbal warning to a dismissal, depending on the gravity of the misconduct and in line with the applicable local laws.

Staff members are encouraged to point out instances of noncompliance with the Handbook to the HR team. This information will be treated with care and full confidentiality.

In-bound Telephone Calls (VoIP)

Answering the calls to the Zurich Office main line (# 5440) is a joint responsibility of the Sales & Marketing team and HR. The standard phrase for picking up the phone is as follows: “RepRisk, good morning / good afternoon. [This is (name)]. How can I help you?”



All direct lines are automatically forwarded to a voicemail. Voice messages will be forwarded to the responsible parties by the Sales & Marketing team. Detailed information can be found in the Knowledge base of the IT helpdesk.

<https://reprisk.atlassian.net/servicedesk/customer/portal/3/article/676233217?src=-386422725>.

Amendments

RepRisk updates the Handbook continuously. The date of the latest update of the specific policy and procedure is indicated at the header of the respective section.

If you would like to propose a change to any policy or procedure, please send your suggestions to hr@reprisk.com.



Learning about RepRisk

Whether you are just starting at RepRisk, or a seasoned RepRisker, these are the three must-know resources where you can find information about RepRisk, what we do, and how we are organized:

RepRisk Website – www.reprisk.com

On our website, you can find key publicly available information about RepRisk, our history, our products, and our clients.

RepRisk AG Team Site (Further Referred to as “Team Site”)

We use SharePoint as our virtual repository for internal documents. The Team Site is the main intranet site for all RepRisk staff to find information specific to their job, their team, or general office matters, such as back-office templates, processes, or team events and photos. Use Search function if you are not sure where the document you are looking for is stored. In addition to the Team Site, we have several access-restricted sites for specialized documents (e.g., HR, Finance etc.), which certain employees have access to, on a need-to-know basis.

[RepRisk Information Bank](#)

This page contains comprehensive information on all aspects of RepRisk setup, products and operations. Take the time to read it, and you will be rewarded with answers to practically all questions you ever had about the company. Please note that this site is *for internal use only*, and only information that is also found on our website can be freely shared outside of RepRisk.

If after reviewing these resources you still have questions that are not answered, let us know at hr@reprisk.com – we’ll be pleased to assist!



Global Policies and Procedures

Quality Assurance

Last updated: [May 1, 2021](#)

Aim and Quality Level

RepRisk data science is used to identify, assess, and monitor the environmental, social and governance risks attached to companies, projects, sectors, and countries.

For RepRisk as a premium provider to have credibility with clients, it is crucial that we maintain high quality and consistency in the service we provide.

To achieve this, we must ensure all external communication is correct, informative and easy to understand. This is to be reflected in our database and products and in our correspondence with clients, media, and other external parties. If the staff member finds errors in the database or in any working documents, they should get these corrected immediately by either getting the owner to correct it or getting the permission from the owner to correct the respective errors, but only after making sure that they are errors.

RepRisk is a growing company and thrives off your passion and drive for what we do. We encourage everyone to take a pro-active approach to their work and to constantly think of how we can develop and improve.

Double-check Principle

We follow a “double check” principle. This means that important decisions, database entries and all non-routine external communications should always be made with the consultation or approval of a senior member of staff.

Use of Style Guide

We follow the [RepRisk Style Guide](#) for any texts in English, whether in internal operations or in client-facing communications. The RepRisk Style Guide contains English language conventions, such as the use of American English, rules on numbers, date format, punctuation, abbreviations, place names, grammar reminders etc. All staff are required to adhere to the Style Guide and can consult it on SharePoint Team Site.



Use of Templates

We always use RepRisk templates (Microsoft 365 Word, Excel and PowerPoint) when creating new documents. RepRisk templates are available for download from the Team Site and are meant for both internal and external use.

We use a uniform e-Signature for all email communication. Our e-Signatures include the links to our social media assets Facebook and Twitter. Staff member's signature is automatically generated by Microsoft 365.

We should ensure we maintain consistency in formatting and layout of documents.

We should update existing documents when something is out-of-date, e.g., the header or footer or the font.

Communication with Prospects, Clients, and other External Parties

It is extremely important that everyone understands our clients' needs to ensure that our work meets their needs. Everyone should understand our unique selling points and be familiar with how to deal with customer communication.

When sending documents externally:

Check that contents, format, as well as all dates are correct (in the file name, within document, in the footer)

Follow file-naming rules set out in Information Security and Data Management

Follow data confidentiality definitions (mentioned in the footer) and handling rules set out in Data Protection and Confidentiality.

Client Service

To maintain our respected reputation for quality and service it is important to adhere to deadlines agreed upon with our customers. Should the staff member not be able to meet a deadline, this should be communicated to the customer with ample notice.

Customer emails and phone calls should be answered within 24 hours.

Continuity of service must be ensured during leaves and absences, by delegating mailboxes and other duties to deputies and teammates.



Data Protection and Confidentiality

Last updated: July 3, 2023

At RepRisk, data protection is based on the “need to protect” principle, which means that staff has access to all documents except those, access to which needs to be restricted. We have defined several degrees of data confidentiality, which determine levels of restriction on data access and sharing permissions.

Personal and Sensitive Data

Personal data refers to: any information relating to an identified or identifiable natural person. Examples of such data are name, postal address, phone number, title, e-mail address. Staff are expected to inform HR in case of any change in these data. Other personal data refer to applications or performance evaluations and the like.

Sensitive data refers to: information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, criminal or administrative proceedings and convictions.

RepRisk’s Policy on Personal and Sensitive data is as follows:

RepRisk collects personal data but not sensitive data, unless required by local laws

Data is collected for specific, explicit, and legitimate purposes (known to the data subjects)

Data collected will be adequate, relevant, and not excessive in relation to the purposes

Data will be accurate and, where necessary and feasible, kept up to date

Data subjects have a right of access and rectification

Staff can restrict access to their data e.g., so only HR, the CEO, as well as line managers have access (on a need-to-know basis)

Security measures are put in place to protect personal data (e.g., HR files including testimonials, applications, yearly reviews, compensation etc.) as appropriate (e.g., restricted SharePoint site, locked cabinets).

Data Confidentiality Definitions

Please see our [Information Classification and Handling Policy](#).



IT, Information Security, and Data Management

Last updated: [October 15, 2020](#)

Data Management

1. Archiving

RepRisk Business correspondence and documents must be kept for 10 years, even after a staff member leaves the company.

This also applies to emails that are saved and accessible to the line managers and selected colleagues (if applicable) after a staff member leaves the Company.

2. Back-up

The following systems are automatically backed up on a regular basis:

Source code

IT and product development tools (Confluence, Jira, and GitLab)

RepRisk databases

RepRisk Aggregator (pool of identified documents of possible interest for ESG risk analysis)

Microsoft 365 / SharePoint

CRM tools (Salesforce)

ERM tools (Sage)

It is the staff member's responsibility to ensure their working files are backed up if they are not saved in any of the locations mentioned above.

3. Filing

We are a knowledge-based company: our staff and our data are our only assets. Therefore, please file everything very carefully. Please strictly follow the following rules regarding filing and documentation.

Staff has always to work on and store files directly in one of the information systems provided by RepRisk, i.e., SharePoint, OneDrive, JIRA and Confluence. For draft documents, both SharePoint (in a draft subfolder) or OneDrive can be used.

Important: Personal working computers are not backed up.



Keep all folders tidy and only leave current files in there, e.g., the latest or final Word or PowerPoint document and the corresponding PDF file, if any. Move outdated documents to an archive subfolder called "zz_Alt" within the same folder. If no zz_Alt subfolder exists, create one.

4. Naming and Formats

We use the following naming format for all electronic documents:

"6-digit creation date (year, month, day), name of document, underscore, initials of owner/creator"

E.g., 170617 Company Introduction_LCr

Important: Always ensure the date in the file name and the date in the document and footer are the same. Always ensure each document has an owner. The owner's initials are always to be added at the very end of the file name (see example above). You can add the initials of a second owner if necessary.

File and folder names should be self-explanatory. Please use short and concise names and always store files in widely used file formats. Personal documents

The personal work computers are not backed up and therefore all personal documents should be stored in Microsoft 365 OneDrive (personal SharePoint storage space). This storage is private, and files are not accessible by others unless the staff member shares them. Should an employee leave RepRisk, he or she can copy personal documents to a personal storage device and delete them on OneDrive.

5. Sharing of Files and Folders on SharePoint

Internally, documents are never sent as email attachments, but instead are shared. One can do this by:

- 1) Sending a link to the corresponding file location via email. This sharing method ensures that access rights to documents are maintained is therefore preferred.
- 2) Using the "share" function on SharePoint. This option should only be used if the recipient already has access to the file, or – exceptionally – if they are to be granted access to the document.



6. Versioning

When making changes to a document, do not update the file name (creation date, document name, initial of owner): all changes and document versions are automatically archived on SharePoint, making it unnecessary to keep older versions as separate files. The same is true for overwriting PDF documents. Therefore, it is also not necessary to add a version name (never do this) or “draft” to the file name (you can do this exceptionally to make clear to everyone that this is indeed a draft).

7. Review of Documents

Each reviewer usually works on the document in the correction tracking mode (if applicable). It is up to the owner to accept or reject the corrections. Corrections/input from clients and suppliers: Save their original file unchanged in a separate subfolder and then save a new file in a different folder following our naming format.

There is no need to add the initials of the people editing the document as this is also automatically captured by Word/Excel/PowerPoint and SharePoint when working with SharePoint (see above).

8. External Documents from Clients, Suppliers, and other External Parties

Save the original file in a separate subfolder specifying the date of receipt, e.g., 170515 Docs from Robeco.

Do not alter the file name of the original file.

Follow the naming rules above for modified files and save them in a different subfolder.



IT & Software

IT Help Desk

The help desk should be used for all IT requests, including feature and export requests, error reports, login and account issues, Microsoft 365, etc.

Please go to: **<http://it-help.reprisk.com>**

To create a new request, open the help desk in your browser and follow the steps below:

Create a request

After logging in, please send a request by choosing one of the available request types. Fill-in the required information and do not forget to provide as many details as possible. The more information IT gets, the easier it will be to resolve your issue.

For certain types of requests, one can also specify the importance or level of urgency. Please keep the implications of the different priority levels in mind:

Blocker: A system or application is unusable / unavailable, or multiple users / clients are facing severe issues in using one of our systems. These requests have highest priority. IT will immediately take care of such an issue and put all other IT work on hold until the issue is resolved.

Critical/High: Very urgent requests or issues that affect major parts of a system or application, where no workaround is available. IT will take care of such request as soon as possible.

Major/Medium: Requests having normal priority and major functional issues. These requests will be scheduled according to the overall IT planning and available resources.

Minor/Low: Non-urgent requests and issues with an easy workaround in place.

Trivial: Cosmetic problems like typos or misaligned text or other easy-to-fix issues.

In addition to the web-based help desk, it is possible to create help desk requests directly via email: <mailto:it-help@reprisk.com>. However, the web-based application is to be used whenever possible.

Request Processing

The staff member will be contacted by email as soon as your request has been picked-up by somebody in the IT team. Further communication on the request can be done via the web-based help desk application, or by directly replying to help desk emails. The entire discussion thread will be stored in your ticket for future reference.



Request Resolution

IT will inform the staff member as soon as their issue has been resolved. Additionally, employees can always check the status of their requests by clicking on "My requests".

9. Software

All RepRisk computers must have legally purchased software installed.

All RepRisk computers must be regularly updated for security, including anti-virus protection.

New licenses can be ordered by IT upon issuing of an IT Help Desk Ticket.

10. Deletion of RepRisk Related Documents upon Resignation

All RepRisk related documents and e-mails must be stored in Microsoft 365 (SharePoint, OneDrive, emails). In case such documents are saved somewhere else, e.g., on the desktop of the computer, they must be deleted from all devices and any location of storage other than Microsoft 365 upon leaving the Company. A confirmation of the deletion of all documents and e-mails must be sent to Admin/HR by e-mail prior to the last day of work.

11. Passwords

Shared passwords should be made available to the corresponding user group through the Shared Password Tool (<https://passwords.reprisk.com>). New or changed shared passwords should be reported to IT using the IT Help Desk.

Personal passwords should be memorized or kept in a secure password tool. They must never be written down on paper or the like.



Safety

Last updated: [August 10, 2020](#)

RepRisk values a safe work environment and is committed to ensure safe, efficient operating conditions, thereby safeguarding staff and facilities.

The Company will not knowingly permit unsafe conditions to exist, nor will it permit staff to engage in unsafe acts.

Role of Employees

Since the staff on the job is frequently more aware of unsafe conditions than anyone else, employees are encouraged to make recommendations, suggestions, and criticisms of unsafe conditions to their immediate supervisor so that they may be corrected.

Role of Supervisors

Supervisors are responsible for the working conditions within their team and the office generally. A supervisor should always remain alert to dangerous and unsafe conditions to recommend corrective action, discipline employees who habitually create or indulge in unsafe practices, assess new or changed situations for inherent dangers, and follow up on employee suggestions for corrective action so that unsafe conditions are not instituted or permitted to exist.

Illnesses / Injuries

All employees are required to immediately report all occupational illnesses or injuries to your supervisor, no matter how minor, and follow procedures as defined by your local office.

Emergency Procedure

Employees are required to familiarize themselves with the relevant emergency procedure in their local office, and strictly follow it should the need arise.



Environmental Sustainability

Last updated: [August 10, 2020](#)

RepRisk is committed to minimize its environmental impact by complying with environmental laws and regulations, promoting awareness among staff, and implementing actions for continuous improvement.

Commitments

Reduce office energy consumption (e.g., heating, lighting, computers)

Reduce office water consumption

Avoid or significantly reduce office paper consumption

Minimize and compensate staff environmental footprint from transportation (e.g., business trips)

Limit use of hazardous chemical products

Minimize waste production and manage waste recycling (where facilities exist)

Increase staff's awareness about environmental issues

Responsibilities

All staff is responsible for implementing the policy, while the management is also responsible for planning, and monitoring the Environmental Sustainability policy and procedures.

Procedures

Energy consumption: turn off all electronic devices prior to leaving the office. Make sure lighting and heating / air conditioning systems are not left on without need.

Paper consumption: As a digital company, we do not use paper for internal documents and communications. If it is necessary to print, make sure you print on both sides.

Environmental footprint from commuting: choose whenever possible the transportation means with lower environmental footprint (for example, public transportation or bike instead of car). We support home office if possible, to reduce commuting.

Office and service suppliers: whenever possible, office supplies such as electronic equipment, food and beverage, and cleaning materials will be chosen based on the



lower environmental impact. We also screen suppliers with the help of our own RepRisk metrics to make sure they do not have an adverse impact on the environment or society.

Waste management: office-based staff are required to follow the waste management rules set up in the Office Rules of your location. Avoidance of waste and recycling are a priority.



Code of Conduct

Last updated: August 10, 2020

Introducing the RepRisk Way

In order to assure the consistency of our services, and thus the success of our company, RepRisk believes it is extremely important that all staff live up to our values, ethical standards, mission, and vision while facing the challenges of their daily activities. In this sense, as RepRisk continues to expand its operations, the Code of Ethics, or "[The RepRisk Way](#)", was developed to put into words the principles that guide the company throughout decision-making. All staff are required to read The RepRisk Way and comply with it.

Safeguarding Personal Rights

RepRisk acknowledges and safeguards the staff members' personal rights and is committed to have due regard for their health and ensure that proper moral standards are maintained. RepRisk is committed to ensure that no staff is sexually harassed, and that any victim of sexual harassment suffers no further adverse consequences.

To safeguard the personal safety, health, and integrity of its staff, RepRisk takes all measures that are shown by experience to be necessary, feasible and appropriate, and which are fair to expect of RepRisk given the employment relationship and the nature of the work.

RepRisk prohibits any form of offense related to someone's safety, health, and integrity, whether physical, verbal, or non-verbal. This includes, among other things, text messages and online conversations. We expect all staff members to be sensitive in the way they approach colleagues and always respect individual privacy.

Feedback Process

RepRisk conducts a yearly Inter-Departmental Feedback Survey and a Company Wide Survey as additional tools to collect criticisms and to flag and address relevant issues related to the Company's code of conduct. Therefore, we encourage all staff to give valuable feedback.



Gifts and Entertainment

Last updated: [August 10, 2020](#)

Giving or accepting gifts and entertainment are commonly used as a form of courtesy when strengthening working relationships with external parties such as clients, suppliers, and government administration. However, if not handled carefully, they may also create the appearance of making an inappropriate influence on external parties, which could impact the company's reputation in the market.

The policy applies to all staff and agents acting on behalf of RepRisk.

General Rule

Staff must ensure that the provision and receipt of gifts:

- Does not create the appearance (or implied obligation) that the gift giver/recipient is entitled to preferential treatment, better prices, or improved terms of sales/purchases
- Would not impact the reputation of RepRisk or the gift giver/recipient if disclosed publicly
- Is not valued at more than the equivalent of CHF 50 (except for flowers)

The following gifts are never appropriate:

Gifts of cash

Gifts that are prohibited by local law

Gifts given as a bribe, payoff, or kickback

Gifts the recipient knows are prohibited by the gift giver's organization

Gifts given in the form of services or other non-cash benefits (e.g., the promise of employment)

Responsibilities

All staff are responsible for implementing the policy, while the management is also responsible for defining and monitoring the Gifts and Entertainment procedures in their local office.



Key Company Processes

Last updated: [July 3, 2023](#)

This Section contains information on the key Company processes, which concern all RepRisk staff. This Section outlines the globally applicable standards and rules, which are further detailed and implemented at the local office level.

Recruitment

All job openings are announced during the Global Team Meeting and are advertised on the company's website and in the applicable local and/or international channels. Staff are highly encouraged to propagate the news among their acquaintances.

Hiring decisions are made by the line manager responsible for the employee in question (hiring manager). Such decisions must comply with the relevant HR policies and require approval by a GLT member. Hiring decisions require at least two interviews with two separate interviewers. The designated recruitment team consisting of the hiring manager and HR jointly take decisions on advancing candidates through the assessment process. A background check on the final candidate must be done before finalizing the employment contract, which usually consists of a documentation check (academic credentials, reference letters, work authorization), as well as a reference check.

Following the hiring decision, the recruitment team must communicate formal feedback to all applicants who submitted their candidacy.

Contact information and all related candidacy documents are restricted and must only be shared with staff directly involved with the recruitment process.

New Hire Onboarding

Once the offer is accepted by the selected candidate, the relevant line manager provides HR with the agreed-upon terms, and HR coordinates issuance and signing of the employment contract. The New Hire Checklist form guides new staff members in their onboarding and integration.

Yearly Objectives

At RepRisk we strive to maintain a performance-driven culture. One of the tools for that is our Yearly Objectives (YO) process.



All RepRisk staff are required to agree with their line manager on their yearly objectives, which are recorded using a YO template. Apart from performance objectives, this document also includes agreement on development goals, and training plans, if any. This document is then used to assess progress and achievements, first at a mid-term review, and then at the year-end assessment.

The Yearly Objectives cycle is as follows:

Defining YOs: January – February

Mid-term review: June – July

Year-end reviews: December – January

Internal Meetings

Mandatory internal meetings include:

The Global Team Meeting, where the whole RepRisk global team meets once per month for a session consisting of team updates, company updates, and deep-dive presentations in various topics of staff interest

Local office meetings

And any other meetings as may be defined by each department

It is part of the staff member's responsibilities to attend all scheduled meetings and conference calls punctually and well-prepared.

An attendee must notify their respective line manager in advance in case they are unable to attend. If an attendee is late to a meeting and their presence is not vital for the meeting to take place, the meeting should go ahead regardless of their presence at the scheduled time.

When joining an online meeting, each participant must ensure:

A good internet connection

A good microphone/speaker system (headset preferably) and video camera

A quiet environment

The mic should be muted during the time other people are speaking (in meetings with large groups)

If one gets disconnected from a meeting, a colleague in the meeting (NOT the chair of the meeting) to add him/her to the meeting or discreetly inform the chair if necessary.

Inter-departmental Feedback and Company-wide Survey

To enable staff to help each other grow as professionals, and to provide a regular channel for staff to give feedback to the company, the following two structured feedback surveys are conducted across RepRisk once a year:

- 1) The Company-wide Survey is meant as a key channel for our team to share the feedback about their experience working at RepRisk. All submissions are anonymous, and aggregated results are shared back with the team. Everyone's participation in the Survey is highly encouraged.



2) Inter-departmental Feedback allows each of our staff to give and receive feedback to/from their teams and colleagues across the company. Aggregated feedback is communicated to the staff by their supervisor as part of the performance discussion.

HR team coordinates both these processes, analyses and presents received feedback, while protecting anonymity of participating staff.

Raising Issues and Getting Support

In addition to the above two feedback processes, if a staff member needs to raise a personal issue, bring up a complaint, or suggest an improvement, they have a choice to contact:

Their respective line manager, or

Their HR support at the local offices, or Ivana Suter, the Senior HR Specialist at HQ.

The HR team are specifically tasked with providing such HR support to all RepRisk staff. Depending on the situation, they would do the necessary follow ups, and come back to the staff member with feedback and/or next steps. They ensure that privacy of the issue and the person remains intact and pre-align with the person in question any disclosure to other stakeholders in the Company.



Training Policy

Last updated: [August 10, 2020](#)

RepRisk supports teams' learning with training time and, where necessary and possible, financial support. All staff are entitled to a basic training allowance, whereby up to 2 standard workdays (pro-rated for part-time staff) spent on training and development per year can be counted as work time. Additionally, a \$50 contribution towards training fees can be paid directly or reimbursed by the company.

Conditions for taking advantage of the above basic allowances are:

Training must be job-relevant

Training needs to be agreed on with the line manager

Training needs to be part of the yearly objectives (YO) as an agreed-upon activity to support Development Objectives

Learning should be followed up in YO reviews, integrated in the job, and where relevant shared with others in the team

Additional training allowances (time and/or financial contribution) can be requested via the line manager to the Division Head but are subject to prioritization. These are usually prioritized among Division Heads based on budget available, the company needs, and internal equity considerations.

Online learning is the most accessible and flexible training format. A list of suggested online learning / Massive Open Online Courses (MOOC) platforms can be found on the RepRisk Academy Site under [Online Course Platforms](#).



Global Mobility

Last updated: [November 15, 2022](#)

Please align with your line manager and head of department, and then contact Human Resources at hr@reprisk.com with your request.

Media and Communications

Last updated: [May 1, 2021](#)

Please refer to the [RepRisk Media Policy](#)