Guidelines and user rules for Securitas Workplace

Version 3.0 (last updated 2021-01-31)

Introduction

These guidelines and user rules are intended to facilitate learning and information exchange on Workplace. The guidelines and rules apply to anyone who has a user account on Securitas Workplace.

As a Securitas employee, you set an important example for your colleagues. Workplace gives you the chance to tell your story and to create interest in your work. Everyone who has access might have a different view on the benefits of Workplace. However, your contribution is considered important as your knowledge and experience can mean a lot to someone else. It can be an opening to new contacts and an exchange that benefits you as well; there's a good chance that you'll find like-minded people to interact with who share your interests.

In other words, Workplace can help you find inspiration, news and facts about subjects that interest you and are relevant to your field or role. Next to that you will find information about the strategy of the company and updates from the CEO.

Workplace brings the world close together and allows you to be in direct contact with your colleagues around the clock, but don't expect that everyone will answer you immediately.

Much like other social contexts, you will get the most out of things by being polite and accommodating. If you would not say or do it in the break room or at the coffee corner, don't say or do it on Workplace. Everyone is responsible for maintaining a civil, constructive and productive tone in the groups and discussions. **Always connect with respect.**

Do's and Don'ts

Do...

- Complete and update your Account (add a picture of yourself)
- Strive to be clear and understandable when you post
- Be personable in your communication, but remember the difference between personal and private.
- Invite others to participate in dialogue and discussion. Comment on and otherwise acknowledge others' posts.
- Respond to the interest others show in you and what you've written.

- Speak up respectfully if you think someone might be wrong or misinformed.

- Respond to those who show interest and engagement when you pose questions or ask for input.

- Use emojis ☺ to add nuance and clarification to what you write – this can reduce the risk of unnecessary misunderstandings.

- Share thoughtfully. What you share becomes a representation of yourself and of Securitas.

Don't…

- Post, publish or share
  - discriminatory content, slander, mockery, personal attacks, insults, threats against ethnic groups, sexist remarks and other harassment
  - unlawful descriptions of violence and pornography
  - criminal requests
  - messages, texts, photos or videos presenting Securitas, its employees, clients or suppliers in a wrong or bad light (see also under paragraph on User rules)

- Use profanity and upsetting remarks.

- Post gossip or unverified information and don't be a spammer
  Publish personal information about colleagues and share photos of your colleagues without first obtaining their permission.

- Argue on political or religious statements that have no direct bearing on our operations.

- Use Workplace to talk about what you do in your free time – this is, above all, a work tool.
- Use Workplace for campaigns, fundraising or lobbying or making money out of selling objects or ideas.

- Share irrelevant or purely personal posts in a group; the latter belong on your own timeline. Respect a group's description and purpose.

- Start group chats for entire regions or businesses. You're welcome to use the chat function to communicate with individual colleagues in small groups, but don't send general messages to large groups of people who aren't expected to answer or respond in any way.

User rules

Information security and the importance of operational security

Workplace is an internal Securitas platform and only employees have access to what is written and published there. Because it's used on private devices, there's a larger risk than with traditional internal communications systems that unauthorized persons can gain access to the platform; someone can lose their personal phone that isn't password-protected, for example.

Everyone must be aware that, certain information can hurt our clients or in the wrong hands. For that reason, it's forbidden to publish secret or sensitive information on Workplace (specified further down in the document). All users need to be aware of this, and it's every user's responsibility to maintain our information security by reminding their colleagues about the following rules.

Anything that breaks the rules should be reported immediately to the system administrators by flagging the post (click on the three dots in the upper right corner of the post and choose "report post".

- Publishing private information is not allowed, whether about how we work or about our clients; only *public* and *internal* information is permitted. *Public information* is factual information published freely within and outside Securitas (such as policies and press releases); however, *internal company information,* retains a certain amount of sensitivity for Securitas (documents in our management system, among others).

- You may not publish or share *sensitive information* regarding the business, our work and other employees. This can include prices and contract information, business strategies, instructions regarding work practices or equipment, etc. A rule of thumb: if we don't talk about it openly, don't post it on Workplace.

- Don't publish client information on Workplace. It's no secret that certain businesses or organizations are our clients, but we never discuss the services we provide or how they're staffed. Don't post about events at a specific assignment, either. Instead, talk about your experiences without identifying the client.

- Publishing pictures taken inside our clients' property or in the surrounding areas is not permitted. Exceptions are pictures taken from places accessible to the general public, for example, a picture of a store taken from the customer parking lot.

- If you want to discuss vacancies: create a group that consists of interested parties or use Work chat; instead of the client's name, use something like position codes or districts/shift-ID.

- Information in the form of text, pictures and videos that have been published on Workplace may not be copied, shared, displayed and in any other way made accessible to anyone outside of Securitas.

- Your login credentials may not be shared with anyone else and should be protected as a valuable piece of information; likewise, you should ensure that you are logged out of any devices before leaving them unattended.

- So that everyone can understand what the conversation is about, only the official language/languages in your respective country are permitted in posts. Preferably use English in the global [ALL] and international [INT] groups; however you can write in your native language, relying on the Workplace translation function.

- The group's administrator is also responsible for ensuring that the group's members follow the guidelines.

System administrators can see the content posted in every group – even groups that are private or secret.

Note that if you don't follow the guidelines, disciplinary action in accordance with Securitas' group and local policies may follow immediately. Failure to comply with these guidelines will be reported to your immediate supervisor and your account may be deactivated.
In addition to the guidelines and user rules above you must accept **Facebook's own Terms of Use**
https://securitas.facebook.com/work/legal/FB_Work_AUP/?show_chrome=false