Cybersecurity Rules for Suppliers

INDEX

REVISION HISTORY

Revision	Chapter/paragraph	Date	Description
1.0		01/04/2024	First release
2.0	Section '4. Definitions'	01/11/2025	• New definitions added for Corporate and Private Data;
	Section '6.1. Acceptable Use of Ferrero Instruments including Backup' and 'Email' sub-sections		• New rules about 6.1.6 "Data Storage" grouped within a new section with guidelines to logically secure the use of storage devices added, and 6.1.8 How to securely store or share corporate information.
	Section '6.1.9 Generative AI'		• Content about "Business Use of GenAI Tech Sites or Platforms for a Project" has been removed to refer to the new Group AI Policy • Name *"Bing Chat for Enterprise"* with *"Copilot Chat"* (by MS), updated
	6.1.10.2 Phishing Awareness Campaign and Consequences Management Framework		• New procedure for guest users who experience sequential compromises during phishing simulation campaigns
	Section 6.3 'Cybersecurity Incident Reporting'		• Updates with more detailed information

1. OBJECTIVES

The objective of the Cybersecurity Rules for guest users is to protect Ferrero guest users, partners, and Ferrero information assets from illegal or damaging actions by individuals, either knowingly or unknowingly.

This document outlines rules for Ferrero guest users to ensure compliance with the security principles stipulated in other Ferrero policies, namely, accountability, authentication, availability, confidentiality, integrity, need-to-know, non-repudiation, and resilience. It further describes the security and compliance checks which may be carried out by Ferrero to confirm that these rules are complied with, and to allow the company to react to any security incidents which may arise.

Inappropriate use of Ferrero instruments and information exposes the company to risks including attacks from internal or external threats, compromise of network systems and services, and legal penalties.

Effective security is a Ferrero effort and a shared responsibility, involving the participation and support of every Ferrero guest user and affiliate who deals with information and/or information systems. It is their duty to know these rules, and to conduct their activities accordingly, in alignment with the *'Ferrero Code of Ethics'*.

2. SCOPE

The scope of this document is to:

- Make certain all use of Ferrero resources is aligned with these rules and is done in a secure way for appropriate business and personal purposes;
- Highlight logical access controls;
- Underline the Cybersecurity incident reporting;
- Explain the interventions, security and compliance checks that may be carried out in Ferrero.

A description of each area is outlined in section '6. OVERVIEW' below.

3. APPLICABILITY

This document is part of the Information Security Management System that governs Ferrero processes and operations within the Cybersecurity context.

The rules defined in this document apply to all Suppliers of Ferrero Group entities, companies, affiliated and business units, without exception. It is mandatory that those who engage in work for Ferrero or use Ferrero Instruments, whether as a guest user, a contractor, a consultant, or a supplier, adhere to, consult, and comply with these rules.

4. DEFINITIONS

Acceptable Use Policy: Topic-specific policy that establishes the information security requirements for protecting and handling Ferrero's information and other associated assets. It provides clear directions on how personnel and external party users, using or having access to such assets, are expected to use them.

Classified Data: Ferrero data assigned by the information owner with a label of CONFIDENTIAL or SECRET based on the potential damage that would be caused to the Ferrero Group if the "confidentiality" would be compromised.

Confidentiality: Property that Ferrero information is not made available or disclosed to unauthorized individuals, entities, or processes.

Corporate Data: any Ferrero information generated and / or collected during Ferrero operations. It includes information on companies, such as financials, operations, and governance, supporting business analysis and activities.

Cybersecurity Incidents: Any cyber event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits; or that constitutes a violation of Ferrero regulations, whether resulting from malicious activity or not (e.g., a successful login recognized as malicious, among a series of login attempts).

Device: A piece of equipment, such as a printer or disk drive, designed to serve a special purpose or perform a special function.

Ferrero Instruments: Email, computers, and devices with information storage capability provided by Ferrero to guest users, to perform Ferrero job-related activities. Examples are PCs, printers/copiers, and fax machines. The category of Ferrero instruments also includes Ferrero mobile instruments.

Ferrero Mobile Instruments: Portable mobile devices with information storage capability provided by Ferrero to its guest users to communicate or access Ferrero resources (e.g., mobile phones) inside or outside Ferrero's physical locations. Examples are laptops, smart phones, tablets, etc.

Generative Artificial Intelligence (GenAI): refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. GenAI can create a wide variety of data, such as images, videos, audio, text, and 3D models applying learning patterns from existing data and then using this information to generate new and unique outputs that typically require human intelligence - *such as recognizing speech, understanding natural language, making decisions, and playing games.*

Guest Users: Third parties (contractor, sub-contractor, vendor/provider) who directly use or are intended to use Ferrero resources.

Guest User Account: unique user account created in Ferreronet for third party personnel.

Information Asset: Any physical or digital information that has value to Ferrero. This term includes elements like software, services, information, and characteristics like skills and knowledge. It can exist in many forms, like printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown in films, or spoken in conversation.

Information Security Management System (ISMS): Management framework for planning, implementing, maintaining, reviewing, and improving information security.

Need-to-know: Principle that states that users should have only as much permission as they need to carry out their duties, to prevent unauthorized manipulations beyond their tasks.

Network: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Personal Data: Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Personal Data Breach: Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data transmitted, stored or otherwise processed.

Phishing: A digital form of social engineering to deceive individuals into disclosing sensitive personal information through deceptive computer-based means. *Note*: Phishing attacks may masquerade as *a lottery organization or the Guest User's bank informing the recipient of a large win*; in either case, the aim is to obtain account and personal identification number (PIN) details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.

Private Data: Any information relating to the private life of a guest user, Ferrero employee or individual, and/or is used exclusively for private purposes. Private Data typically includes correspondence with family members or friends, personal activities or appointments, family pictures, and other non-work-related information.

Sensitive Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.

Spam: Unsolicited advertising.

System: A set of IT assets, processes, applications, protocols, and related resources that are under the same direct management, function, or mission objective; have essentially the same security needs; and reside in the same general operating environment. *Note* that systems might not be owned, hosted, and/or managed directly by Ferrero. Furthermore, systems might not be used by Ferrero employees or guest users, but only owned, hosted, and/or managed by Ferrero.

Third Party: external person or entity such as contractor, sub-contractor, or supplier (including consultants), that in case of need will be provided with a guest user account in Ferreronet.

5. COMPLIANCE

Compliance with these rules is mandatory and should be enforced by the Ferrero Group and Local management within their divisions.

Failures to comply with these rules are grounds for the application of disciplinary actions, according to applicable national legislation and without prejudice to the possible adoption of other measures related to responsibilities of any other nature. Ferrero may initiate these actions as a result of failures by Guest users to comply with these rules, which are detected during ordinary or extraordinary controls. Data analyzed during these controls may be used as evidence to support such actions.

6. OVERVIEW

6.1 Acceptable use of Ferrero instruments

6.1.1 Ferrero instruments

- Ferrero instruments are leased by or property of Ferrero and are assigned to guest users, who are responsible for their secure use, safety, and integrity.
- The use of these Ferrero instruments by guest users is for professional purposes (the performance of the task assigned to guest users by Ferrero).
- The use of Ferrero devices and assets is strictly limited to the assigned Guest user. It's forbidden to extend the usage of devices and assets to other third parties individuals.
- Guest users are not allowed to install or distribute any software products that are not appropriately licensed for use and do not comply with the software restriction rules defined by Ferrero. If required by their scope of work and aligned with the respective Ferrero responsible, installation of additional software shall be preliminary validated by Ferrero IT and Cybersecurity.
- Guest users are not authorized to access, store or disseminate pornographic content or offensive material (e.g., racist, sexist, etc.) in any Ferrero instruments such as computers, peripheral devices, connected storage devices, or mobile phones.
- Ferrero instruments are equipped with dedicated protection systems. Suppliers are not allowed to change or modify these system protections.
- Ferrero IT department is the sole authorized to carry out maintenance on devices and assets. It's therefore forbidden to seek technical support from external providers without prior authorization of Ferrero IT.
- Suppliers are required to comply with local legislation, and not to act and/or behave in a way that might involve danger and/or damage to networks, systems and applications, or impact on other users.

6.1.2 Clear Screen and Desk

- Guest users must lock their PC whenever they leave their workstation, even if it is only for a very short time (press keys CTRL + ALT + DELETE and then click Lock Computer in the windows security dialog box; or press Windows key + L).
- Guest Users are responsible for turning their Ferrero PC / laptop off once they have finished working.
- Guest users are responsible for applying the security patches suggested by Ferrero IT to keep their Ferrero instruments up to date. If Guest users receive a notification that the Ferrero instrument needs to restart, they should do so as soon as possible, otherwise they should shut down their Ferrero instruments upon completion of work to ensure the updates are installed.

- Inside and/or outside Ferrero facilities, Guest users must ensure that when entering their passwords or working with confidential information, these cannot be seen on their screens by other individuals; and that confidential conversations cannot be eavesdropped by unauthorized persons.
- Ferrero confidential information on paper or electronic storage media that should be deleted must not be left unattended; they must be secured until they can be securely disposed of, following the media sanitization rules defined by Ferrero.
- When leaving a Ferrero meeting room/office, guest users must turn off external devices such as video conference systems, clear desks of all papers, notes and/or any documents, remove/wipe all Ferrero confidential information that might be written on a flipchart, whiteboard, papers, or technical whiteboard devices.
- The handling of Ferrero corporate data on removable storage devices must follow the rules defined by Ferrero to classify and manage Ferrero information.
- Ferrero information media, storage media (e.g., hard disks, USBs, etc.), and generally information in printed form containing Ferrero classified data shall be physically secured in locked drawers or cabinets when not in use, especially outside of office hours.

6.1.3 Printers, copiers, fax, and document shredders

- Ferrero printed documents must not be left unattended on printers/copiers/fax devices; instead, they must be withdrawn immediately by the owner.
- The usage of Ferrero printers and copiers to duplicate, even partially, any material protected by copyright – without previous authorization of the Ferrero owner – is explicitly prohibited.
- Any Ferrero document sent to a third-party printer should immediately be printed, and if not needed anymore must be deleted, or purged from the print queue and from its internal HDD/memory.

6.1.4 Ferrero Mobile Instruments

- Only Ferrero Mobile Instruments approved by the Ferrero IT department, acquired through the Ferrero corporate purchasing process, or authorized by Ferrero, can be used to store Ferrero-owned data.
- Ferrero Mobile Instruments containing Ferrero information must be kept in a secure place. It is strongly advised to keep them inside the office in a secure storage location (for example, a locked drawer, desk, cabinet, or a controlled media library).
- In case of loss or theft of a Ferrero PC, Ferrero mobile phone or any Ferrero mobile instrument, guest users must inform immediately the Ferrero IT department and personally report the loss or theft without undue delay to the Police Department competent for the jurisdiction where the event occurred, if materially possible.

6.1.5 Information management

- Ferrero business relevant information and personal data must be handled according to Information Classification and Privacy and Data Protection rules defined by Ferrero, as well as any applicable regulations.
- Ferrero guest users must process, store or share corporate information only through the Ferrero IT ecosystem provided by the Company to them (Microsoft O365 suite). It's not allowed the use of alternative communication channels such as private email (outside Ferrero management), or other communication platforms such as, but not limited, to iMessage, WhatsApp, Telegram, WeChat, Signal, etc. to process, store or share Ferrero information.
- Ferrero IT department is not responsible of any activities linked to the management of the data stored in the folder called "Private Documents – Not Protected" on guest users Ferrero PC.
- Ferrero guest users must not publish images, videos, etc. related to their **confidential** job activities at Ferrero, Ferrero **restricted areas** (e.g., data centers, research centers, plants, laboratories, etc.), or related to other third parties who have not been previously and properly informed.
- Ferrero guest users must not share **confidential** details of their job activities at Ferrero, especially through social networks, instant messaging, or other media.
- Ferrero guest users must avoid undertaking confidential Ferrero calls or working on confidential Ferrero documents in public spaces (e.g., trains or airports).
- Personal data, including credit card numbers and bank account details, must not be shared, or otherwise processed without proper authorization to do so.
- It is forbidden to provide information or lists of Ferrero employees, associates, customers, or contractors to other third parties without a verified legal ground for the transfer, and an approved and executed non-disclosure agreement (NDA).
- Any use of Ferrero information protected by or containing any copyright, trade secret, patent or other intellectual property, or similar laws or regulations without authorization or prior consent of the rightful Ferrero owner is forbidden.
- Guest users are required to maintain strict confidentiality of any Ferrero information they get access to for their Ferrero job activities that are not in the public domain, or it has been identified as confidential by Ferrero, at any time, either during or after the termination of the employment relationship with Ferrero. Guest users must handle that information with utmost discretion and take all the necessary precautions to prevent their disclosure, according to the *'Ferrero Code of Ethics'.*
- When dealing with public statements, the guest user must refer to and comply with the Ferrero '*Social Media Guidelines*'.

6.1.6 Data Storage

- To maintain the security and accessibility of the Ferrero data, it is essential to store it in the designated Ferrero Business Repositories (Desktop, Pictures, or Documents folders), which are synchronized with Ferrero OneDrive for Business, Teams Channels, or SharePoint. This enables efficient collaboration, file versioning, and data retention in case of local data loss.
- To minimize malware risks associated with removable media, Guest users must avoid the use of removable storage devices (hard disks, USBs) whenever possible, use them only when is strictly necessary (e.g. in isolated environments), and prefer the use of Ferrero OneDrive for file storage and sharing.
- Ferrero-related e-mail stored in Ferrero Outlook PST *(Personal Storage Table)* must be moved (manually or set as an automatic rule) to the Outlook '*Online Archive'*, to be preserved.
- 'Private Documents – Not Protected' folder, and Local folders including those in the "Downloads" folder of the Ferrero PCs, will NOT be migrated during laptop refreshes, upgrades, or reinstallation.

  ***Note**: Guest users are encouraged to use the existing Ferrero support tools (from the Software Center) to identify and manage not protected local data.*

- In case of Guest User departure, it is the responsibility of each Guest User and their Ferrero responsible to ensure the relevant Ferrero data is properly handed over.

  ***Note** that Ferrero company is not liable for any loss of private data stored on Ferrero instruments, and the storage of such data on Ferrero instruments is subject to the limitation stated on section. 6.1.1. The integrity and availability of any such Private Data is not guaranteed by Ferrero. It's forbidden to store Private data on Ferrero devices.*

6.1.7 Backup

- Backup is intended to restore data in case of failure of the Ferrero instruments and/or any IT system, thus guest users cannot copy or ask for a copy, by any means, of the content (partial or complete) of their Ferrero email inbox, their files within the Guest User's OneDrive for Business area, or files stored in Ferrero shared folders outside the Ferrero IT Ecosystem (i.e. on private USB media device, private cloud services, etc.). Those data are considered Ferrero's intellectual property and must always remain in the Ferrero IT Ecosystem, according to the Ferrero data retention rules.

6.1.8 Secure sharing documents and collaboration with internals

- To securely share files and folders with people inside Ferrero, guest users must use only the collaboration tool allowed in Ferrero. Once the collaboration is done, or at any time, guest users can stop sharing and remove access to their files.

- Guest users must review the people attending corporate meetings before letting them in; and should ask permission before taking screenshots or recording Ferrero meeting sessions.

6.1.9 Generative Artificial Intelligence (GenAI)

A. Business Use of Generative AI Technology Sites or Platforms for a Project

Before using specialized GenAI Technology sites or platforms for a project, the initiative must be approved and complied with the *Ferrero Group AI Policy*.

B. Business Use of Generative AI Technology for General Inquiries

- The use of GenAI sites via Web Browser or Mobile Apps (on Ferrero mobiles), is allowed only for general inquiries that don't contain any information in relation with Ferrero, and it is strictly forbidden to input any Ferrero information (*including but not limited to strategy, trade secrets, personal data, confidential information, intellectual property, financial information, marketing, and media, etc.*); as the information received can be biased and must be verified.
- It is not recommended to register on these sites with Ferrero credentials, to reduce privacy risk.
- Ferrero provides the AI tool called 'Copilot Chat' by MS (GPT-4 enriched web results) to the guest users for usage related to Ferrero business, as it provides commercial protection (user and business data protected, chat data not saved, chat data not used to train underlying models, etc.).

C. Personal Use of Generative AI Technology

- Guest users must **not use Ferrero credentials** (Ferrero guest email and password) to access any GenAI technology (*i.e., ChatGPT, Midjourney, etc.*) for personal purposes.
- It is forbidden to upload on Generative AI technology any type of Ferrero information (*including but not limited to strategy, trade secret, personal data, confidential information, intellectual property, financial information, marketing, and media, etc.*).

6.1.10 E-mail

- The Ferrero e-mail account is individual and non-transferable. The guest user is the sole and direct responsible for the actions taken and messages sent in his/her name.
- Ferrero e-mail messages must be sent only to strictly necessary recipients, to respect the "need-to-know" principle and avoid the disclosure of information to individuals who do not need to know it.
- Guest users shall not use the "reply all" option on messages sent to big groups of recipients (*above 30 participants*), unless strictly necessary for the purpose of that communication. Guest users should also pay attention to emails sent to one or more Ferrero DLLs *(Dynamic Link Library),* ensuring that the recipients included in the selected DLLs are the intended recipients for the conversation.

- Guest users are prohibited from using Ferrero instruments for the transmission of unsolicited bulk e-mail with/without attachments, advertisements, or commercial messages.
- If guest users receive unwanted and unsolicited e-mail (known as spam), they should block the sender and must refrain from responding to the sender, to avoid junk e-mail.
- Ferrero electronic communications must be consistent with the '*Ferrero Code of Ethics'*, considering the e-mail messages as formal documents that must respect the guidelines regarding the inappropriate use of the language.
- The dissemination of messages of general interest (internal activities, invitations, sad notes, etc.) must be managed by the Ferrero People Experience and/or People & Organization departments.
- The abusive use of Ferrero electronic mail and distribution lists is not allowed, including the following practices:
    - Insult, threaten, defame any staff member, or send fraudulent, religious, obscene, or harassing messages, either with the intention of compromising information security, disrupting work or threatening Ferrero's reputation.
    - Subscription to dating websites, non-corporate chats or any other type of activities or electronic bulletins that are not strictly related to the professional Ferrero work area.
- Guest users are not allowed to set up auto forwarding rules to their company mailbox or any other third-party mailbox (either internal or external).
- Guest users shall not manually forward Ferrero's emails, attachments, or part thereof (property of Ferrero) to a private email or their company email address with the intent to backup, preserve, extract or maintain a copy of Ferrero business document outside Ferrero's IT Ecosystem.
- If a guest user is unable to access his/her mailbox for a predetermined period he/she shall set up an Out of Office message with the necessary references (name, e-mail address, etc.) of the person (if any) or team who is temporarily in charge of his/her tasks.
- Whenever possible, guest users should share files as a link to a Ferrero SharePoint or OneDrive, instead of as an attachment.
- Some types of files are not allowed to be attached to the Ferrero e-mail for security reasons (e.g., executable files *.exe*). The e-mail system will block such attachments during the dispatch of the e-mail.
- Guest users must exercise extreme caution when opening email attachments received from unknown senders, which may contain malware.
- Guest users must not let the browser save their Ferrero ID and Password on any web-based application, for example when checking the webmail, (e.g., answer NO when an application offers to remember the login information on browser).

- Guest users must log off their Ferrero webmail session before closing the browser in non-company-issued devices.

6.1.10.1 Phishing

- Guest users must avoid clicking on unexpected links. If in doubt, hover the mouse over unexpected links to check if it is legitimate.
- Guest users should not use their Ferrero e-mail address to sign into personal social networks and private related web services.
- Guest users must verify the identity of any person who tries to contact them via suspicious e-mails or calls to request sensitive information.
- If a guest user receives a suspicious e-mail, he/she must:
    - Verify the sender's contact information by checking name, email suffix and telephone numbers on an authoritative source.
    - Call the person in question to clarify the request but avoid using the contacts in the signature of the email. Guest users should use institutional contacts instead.
    - Do not reply to the email, follow any instructions, or provide any information.
    - Be suspicious in case of first contact: if a guest user has already communicated with the sender, the guest user must check if it is the same person.
    - Do not forward the email to a private email account.
    - Click the '*Report Phishing'* button (located in Ferrero Outlook's "Home" ribbon). Any email reported using the '*Report Phishing'* button will be automatically deleted from the Ferrero Guest User's inbox. These emails reported will be forwarded to the Ferrero Cybersecurity team for analysis, who will reply with the outcome of their analysis.
- If there is a legitimate Ferrero business need to access the contents of e-mail messages (*of professional nature*) within the Ferrero email account of a former or absent Guest User, the request must be filed by the Ferrero responsible for the guest user and approved by the P&O, Security and Legal representatives according to the rules defined by Ferrero.
- Ferrero may also access corporate e-mail accounts in connection with extraordinary controls, as noted below (*for reference, see section 6.4).*

6.1.10.2 Phishing Awareness Campaign and Consequences Management Framework

- Guest users with Ferrero guest user email account could receive e-mails as part of the Phishing Awareness Campaign and simulated phishing exercises.

- To reinforce cybersecurity awareness and accountability, a structured Consequence Management Framework can be applied to the guest users who experience sequential compromises during phishing simulation campaigns. The framework is outlined as follows:
    - First Sequential Compromise:
        - The guest user is required to complete an online training module designed to enhance phishing awareness. Follow-up reminders will be sent by email with a frequency of up to twice per week to encourage timely engagement.
    - Second Sequential Compromise:
        - The guest user will be enrolled in more frequent phishing simulation schedule to reinforce learning and improve detection capabilities.
    - Third Sequential Compromise
        - A one-on-one training session will be conducted to address specific behavioral patterns and reinforce cybersecurity best practices through personalized guidance.
    - More than Three Sequential Compromises:
        - An email notification will be sent to the guest user, with their Ferrero responsible in copy. The communication will highlight the repeated compromises and request immediate attention.

6.1.11 Internet Use

- Ferrero is authorized to block internet sites that lead to a cybersecurity or privacy risk, or that may compromise system integrity, availability, or data confidentiality.
- Non-ethical websites that contain sexually explicit, militancy/hate extremist, racist, violent, or other potentially offensive material are forbidden and shall not be accessed. The ability to connect to a specific website does not imply that Guest User is permitted to visit it.
- In case a guest user requires access to a blocked site for business reasons, he/she can send a ticket to the Ferrero IT Help Desk who will check the site and, if necessary, escalate the request to Ferrero Cybersecurity for analysis.
- Ferrero expects guest users to behave professionally and under no circumstances use Ferrero instruments during, or outside working hours to perform the following activities:
    - any form of online gambling, browser games; or
    - streaming of movies (e.g., Netflix).
- It is forbidden to illegally download files or software protected by copyright or other intellectual property rights (e.g., music files, photos, or videos, movies, etc.).
- Guest User Internet traffic on Ferrero instruments is logged for auditing purposes to ensure compliance with the rules detailed.

- Guest users must not attempt to bypass Ferrero's network and/or web filtering/protection (e.g., firewalls, proxies) while using the Ferrero instruments to access the Internet.
- Guest users must not use unauthorized or personal Internet or cloud storage providers for Ferrero business purposes.

6.2 Access Control

6.2.1 Logical access

- Access to Ferrero information systems is granted and restricted to the use and/or support of the intended application and is only granted once prior consent has been given by the Ferrero responsible for the Supplier, considering the:
    - least privilege ("need to know" principle); and
    - segregation of duties
- Access for guest users shall be provided only under a contractual agreement.
- Guest Accounts must be provided with temporary access that cannot exceed the contract period. If applicable, accounts will be configured by Ferrero IT, setting up the expiration date on which the accounts will be disable automatically. Guest account extension must be performed by the Ferrero responsible for the specific guest.
- Access to information systems must be allowed only through an authentication mechanism that grants access only to authorized personnel by means of entering at least a code for user identification (user-id) and an associated keyword (password).
- Access to Ferrero production systems for application developers, technical and operational staff will be granted only if their Ferrero job specifically requires it. The justification for such access must be registered.
- Each guest user is assigned a unique account within Ferrero applications and systems that establish identity.
- Guest users must be uniquely accountable within all systems they access (i.e., no shared accounts or IDs); where possible, each guest user must be identified on all the Ferrero IT systems through a unique ID.
- Display Name for Guest user must be: firstname LASTNAME (Guest).
- Ferrero email address is built as *firstname.lastname@guest."domainname"* based on information provided by the Ferrero responsible. Uniqueness of email address is ensured through adding numbering in case multiple users share the same first and last name. Passwords of default users of information systems must be changed before putting it into operation.
- Ferrero standard accounts cannot be granted administrative privileges on systems. Admin permissions must be assigned to different accounts from those used for regular business activities (i.e. admin accounts).
- Regular Ferrero business activities should not be performed from admin accounts.

- It is not allowed to use, authorized or not, the user credentials (User ID or Password) of another user. The guest user is solely and directly responsible for his/her accounts on the different Ferrero systems (e.g., SAP systems, Ferrero Intranet, etc.).
- Guest users must not use Ferrero credentials in non-business websites or applications.
- Guest users are not allowed to access data, servers, or any accounts for any purpose other than conducting business, even if they have authorized access.
- Guest user must be provided with “strong” identification and authentication mechanisms that must not be shared between multiple accounts. A strong authentication is required for every external connection to the Network.
- Guest accounts cannot be re-used for internal employees.
- Guest User lifecycle (e.g. new request, user extension, user termination, etc.) is responsibility of the Ferrero responsible who must keep the Guest User information updated.

6.2.2 Ferrero Password Use

- Guest users must not share their password or any other form of access credentials with anyone else.
- Guest users are prohibited from sending their Ferrero accounts passwords by e-mail, posting them on social networks, sending them by instant messages or using any other communication channel.
- Guest users must not write down their password, print it, or store it electronically in an unencrypted manner.
- Password change must be enforced automatically at least every 180 days for Ferreronet guest user account and for application local accounts, except for specific security settings of the IT systems.
- Passwords must not be the same as the corresponding user ID.
- The password must be at least 12 characters long and not easy to guess considering the following:
    - at least 1 uppercase character.
    - at least 1 lower case letter.
    - at least 1 number.
    - at least 1 special character.
    - password history must be maintained and doesn’t allow the re-use of the 24 previous passwords.
    - minimum password strength for Ferreronet account is ensured by Azure AD Password Protection (e.g. password should not contain account username, user real name, the company name, company brands’ name).
- The initial password supplied must be changed on first use.
- The minimum validity for a new password is 1 day in Ferreronet.
- Passwords must not be stored in clear text in a readable form, nor written down.
- Password details must be protected from unauthorized read, change and deletion.

- Passwords must not be displayed clearly (in an intelligible form) at any time, including at the point of entry.
- Passwords must not be written into scripts or other programmed such that the principle of individual accountability is bypassed.
- Validation of password change must be made by duplicate entry, and the existing password must be required as input on password change if available.
- Software and files containing formulas, algorithms, and other specifics of the process used to generate passwords or personal identification numbers must be controlled with the most stringent security measures supported by the computer system involved.
- Passwords shall be immediately changed if there is any suspicion of password compromise, and this shall be reported immediately to Ferrero 1st Level support and to Ferrero Cybersecurity Department.
- Rules about password complexity and re-use are applicable also to local accounts and cloud-only accounts.
- When possible, the user should use Microsoft solutions to autonomously manage password change and password reset. The Self-Service Password Reset (SSPR) tool must be used to reset the password of the standard personal account.

Privileged Personal Accounts

- Admin accounts - Password for admin accounts must be at least 14 characters long, other rules remain valid.

Microsoft Cloud Accounts:

- For Microsoft cloud-based users the minimum password length is 8 chars due to technical constraints. However, it's strongly recommended to use 14 chars to be in line with 'Admin Accounts' policy.
- Password complexity is ensured by Azure AD Password Protection, as it is a feature to reject weak and frequent passwords.

6.2.3 Network

- Only approved Ferrero instruments are allowed to be used to connect to the Ferrero Global Network; any exception must be approved.
- Guest users must be sure to use a secure connection when connected to any network with unknown or low security level using Ferrero instruments.

6.3 Cybersecurity Incident Reporting

- Guest users who use Ferrero information systems and services must observe and report any potential cybersecurity issue and potential personal data breach to the Cybersecurity Team. For example:
    - If classified (confidential and/or secret) Ferrero information and/or personal data is (potentially) lost, destroyed, disclosed, or made accessible to unauthorized parties;

- If any unauthorized use of Ferrero information systems has (potentially) taken place;
- If Ferrero passwords or other Ferrero credentials are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.
- If a suspicious e-mail that involves a bank account or financial matter is received on their Ferrero guest email account.
- If any cyber security event or alert occurs on any device (non-Ferrero included) used to interact with Ferrero environment.

- The potential issue must be sent to the Ferrero responsible and Cybersecurity Department (via the e-mail account cybersecurity@ferrero.com) and shared with local or group colleagues, as they may have received feedback already, and wait for further instructions via email, mobile or from their Ferrero's responsible.
- In case a guest user is victim of a cybersecurity incident he/she must avoid shut down the system or unplug it from the network or electricity. Guest users should neither unplug any external device (i.e. USB) from the system, lock the screen, post social media or share information on the situation or try to fix the problem on his/her own.
- Guest users might be reached by Ferrero Cybersecurity via Teams channel, or Ferrero guest email, or their own company's email asking for cooperation for specific events or security alert. Presence on such communication mediums is mandatory.
- Guest users might be invited by Ferrero Cybersecurity to cyber-incident coordination calls (called WAVEs) to provide information about the issue.

6.4 Interventions, Security and Compliance Checks

To guarantee an adequate security level for Ferrero Group, guest users are responsible for the integrity of the configuration of the Ferrero instruments. Any modification thereof, including but not limited to, installation or removal of Ferrero software eluding security controls and changing security and network parameters without Ferrero's authorization are strictly forbidden. Security resources are in place to protect Ferrero systems and networks, guarantee business continuity and safeguard business information, personal data, and private information from theft, unauthorized access, misuse, and tampering. In the event of any incident, or reasonable evidence of non-compliance with Ferrero policies and local regulations by guest users, the designated departments (Cybersecurity or Group Security) will be allowed to access the Ferrero instruments involved in compliance with data privacy criteria.

The primary goal for the security and compliance checks of Ferrero's network and systems is to protect Ferrero's information assets. Limited Ferrero employees within the IT department, which have been appointed as system administrators, or responsible in Ferrero Cybersecurity or Group Security departments are authorized to carry out interventions on the Ferrero Network and systems for the following reasons:

- To safeguard Ferrero's information assets and ensure the correct use of the Ferrero instruments provided to Ferrero Guest users.
- To safeguard and maintain Ferrero's business continuity and normal business operations.
- Guarantee the security and the operation of Ferrero's network and system, as well as for other technical/maintenance reasons (e.g., replacements or installation of software, hardware maintenance).

To prevent and investigate any acts or events with the potential of criminal and/or disciplinary relevance, or which may amount to breaches of contractual obligations, which may be committed by Ferrero Guest users or others, and which may harm Ferrero, as well as to defend and exercise Ferrero's rights in court, where necessary. These interventions may involve the compliance check of activities carried out on the Ferrero network and on Ferrero's resources by Ferrero Guest users and others. They may be carried out even when a Ferrero Guest User is absent or otherwise unavailable. This set of controls will not be carried out, under any circumstances, to monitor the habits, opinions, or work performance of any Ferrero guest users.

Technical interventions (aimed at providing technical assistance, protection against viruses and malware and, in general, ensuring that business proceeds as normal) may be carried out remotely by the Ferrero's IT or/and Cybersecurity department, with the approval of the Ferrero instruments' owner or guest user, in case the operation requires the view of the desktop. This will happen at the request of the Guest User, where the Ferrero IT or Cybersecurity department confirms an objective need to perform an intervention to solve a detected technical issue. Where not done at the request of the Guest User, they will be notified in advance of the intervention, as long as this does not affect the timelines and effectiveness of it.

General security and compliance monitoring activities may take two forms: ordinary controls and extraordinary controls. These activities will be carried out in compliance with applicable data protection principles, in particular: **lawfulness** (Ferrero ensures that it has a legal basis to carry out such activities, based on its legitimate interest of protecting the security of its information assets and network), **proportionality** (Ferrero will ensure that any impact upon Guest users is not unreasonable, considering the security interests which Ferrero seeks to protect) and **data minimization** (Ferrero will only access and collect the minimum amount of personal data needed to meet these goals).

6.4.1 Ordinary controls

- Duly authorized personnel from Ferrero IT or/and Cybersecurity department may carry out preliminary ordinary controls over the use of the entire Ferrero resources; these controls will be carried out through event logs and alerts.
- Any processing of data in event logs and alerts will be carried out on an anonymous basis (so that the actions observed are not traced back to an individual guest user) or, in any case, in a collective manner or regarding a sufficiently large group of guest users (so that no individual guest user's activities may be identified).

- The purpose of these controls is to allow Ferrero IT and/or Cybersecurity department to monitor the activities carried out on the network in a broad manner, to detect any potential irregularity, incident or threat, while avoiding an excessive intrusion into the privacy of guest users.
- When an anomaly is detected, if appropriate, Ferrero IT or/and Cybersecurity department may:
    - Send out a generalized notice to the Ferrero guest users, with instructions and tasks to be followed to resolve the issue.
    - Send out a targeted notice to certain functions or departments in Ferrero related to the anomaly, which was detected, with instructions and tasks to be followed to resolve the issue.
    - For more severe anomalies, trigger extraordinary controls *(see below).*

6.4.2 Extraordinary controls

- An extraordinary control may be initiated by duly authorized personnel from Ferrero IT and/or the Cybersecurity departments where this is strictly necessary (i.e., where an ordinary control is objectively insufficient):
    - To ensure compliance with this document and the applicable laws and regulations.
    - To manage security incidents. To detect, prevent or remediate actual or suspected unlawful acts, acts with criminal or disciplinary relevance, or acts, which may amount to breaches of contract, carried out by guest users or other third parties.
- During an extraordinary control, duly authorized personnel from Ferrero IT and/or Cybersecurity departments (with the authorization of Ferrero P&O, Group Security and Legal departments) may access Ferrero servers and the storage of any Ferrero resource used by guest users, including any activity logs related to those servers and resources (tracing activities logged back to individual guest users) and any files and data stored on those resources. Log correlations may be also used to detect anomalous behaviors such as data leaks or data theft as a result of risky user activity.
- Guest users should be aware that these extraordinary controls may allow selected personnel within Ferrero IT and/or the Cybersecurity departments to access to incoming and outgoing e-mails traffic within Ferrero e-mail accounts. However, any analysis of e-mail contents and attachments will be only carried out where it is considered objectively insufficient, to meet the goals of the extraordinary control, to merely rely on e-mail metadata (e.g., sender, recipient, subject, date/time of sending).
- The Ferrero Cybersecurity team can reach the guest users via chat, email or phone to have more details about the incidents.