Legal | Policy Area

MEETING RECORDING POLICY

Policy Statement

It is the policy of Qorvo that any video meeting may be recorded or transcribed by automated means when the following conditions are met:

1. There is a legitimate business reason for recording or transcribing the meeting and the employee, exercising their business judgment, expects that recording the meeting will bring more benefit than risk to Qorvo or Qorvo customers.

2. No participant in the meeting objects to the recording or transcribing. If the meeting being recorded or transcribed is with non-Qorvo participants, the participants must affirmatively consent to the recording or transcribing.

3. No participant in the meeting could reasonably be surprised that the meeting is being recorded or transcribed, because it was announced before the recording or transcribing started, either during the meeting or in the email invite/announcement for the meeting.

4. The recording, transcribing, and/or analysis is only being done on an Approved Platform.

5. The recording, transcribing, and/or analysis is only shared with those having a legitimate business reason for accessing the content.

6. The content of the meeting is not a Restricted Meeting.

Additionally, it is the policy of Qorvo that a video meeting—once recorded or transcribed, or while being recorded or transcribed—may be analyzed, summarized or processed in any way through automated means, only if the platform for doing so has been approved by Qorvo's AI Governance Committee and the user is permitted by IT to utilize those functions on an Approved Platform.

While certain meetings with information subject to ITAR or EAR may be recorded or transcribed, nothing in this policy removes the obligation from individuals to make sure that such information is not accessible to those unauthorized to access it.

It is the policy of Qorvo that meeting recordings or transcription should expire after thirty (30) days by default; however, for a legitimate business reason, recordings or transcription can be kept longer. If a recording is needed for longer than thirty days, the person making the recording will be responsible for changing the default expiry. No recording may be kept indefinitely without approval from Legal.

It is the policy of Qorvo that managers should not record 1:1 meetings with their team members, specifically performance reviews or employment related meetings without the approval of their Human Resources Business Partner.

Finally, it is the policy of Qorvo that only the functionality within an Approved Platform designed for recording the entirety of a meeting may be used to record meetings, unless explicitly agreed to by the other participants in a call. Specifically, use of screenshots, screen-capture, screengrab, and other tools not labeled by the Approved Platform for recording a meeting are not permitted without such explicit agreement.

Approved Platforms for Recording Video Meetings

The following platforms are Approved Platforms to record video meetings:

- Microsoft Teams.
- WebEx, but only to support customers requiring the use of non-Microsoft Teams software.

Approved Platforms for Automated Transcribing Video Meetings

The following platform is an Approved Platform to transcribe a video meeting:

- Microsoft Teams.

Approved Platforms for Automatedly Analyzing, Summarizing or Processing Recordings or Transcriptions of Video Meetings

The following platform is an Approved Platform to automate analysis of, summarize or process the recording or transcript of a video meeting:

- Open AI's Enterprise Version of ChatGPT. Use of the free version is ***not*** permitted.
- Microsoft Teams and Microsoft 365 Copilot.

Restricted Meetings

The following are Restricted Meetings and may not be recorded or transcribed:

- Any meeting or portion of a meeting discussing Restricted Personal Data, as defined in Annex I.
- Any meeting or portion of a meeting discussing Controlled Unclassified Information or Classified Information.
- Any meeting or portion of a meeting discussing undisclosed, consolidated financial results for company reporting requirements.

Amendment

This policy is effective on May 21, 2024. Amendments to this policy, including approval of new platforms for recording, transcribing, automatedly analyzing, or summarizing a video meeting or removal of approval for the same, will be reflected in this document and will be immediately binding. Employees are expected to consult this document regularly to confirm whether changes have been made.

Version Table

Date	Description	Author
May 21, 2024	Document Created	Peter McClelland

Annex I

"Personal Data" means information, data, derived/inferred data or any unique identifier that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an individual or household or to a device that identifies, is linked to, or is reasonably linkable to one or more individuals.

"Restricted Personal Data" means Personal Data that includes an individual's:

(A) Social security, driver's license, state identification card or number, national identification number, or passport number.

(B) Financial information, which shall include an individual's account number, financial account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) Precise geolocation meaning data that accurately identifies within a radius of 1,750 feet an individual's present or past location, or the present or past location of a device that links or is linkable to an individual or any data that is derived from a device and that is used or intended to be used to locate an individual within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.

(D) Racial or ethnic origin, citizenship or immigration status, national origin, religious or philosophical beliefs, or union membership, or status as a victim of crime.

(E) The contents of an individual's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual.

(G) Is a child's (under thirteen years of age) Personal Data.

(H) Personal information collected and analyzed concerning an individual's health, individual health data, or data revealing mental or physical health condition (including pregnancy), treatment, or diagnosis.

(I) Sex life or sexual orientation or sexuality, status as transgender or nonbinary.