Encryption process information application and usage guidelines

(Date of release: April 19, 2019)

I. Workflow: Approval of application documents → pass an information security field audit Completion of information security course and examination → granting permission to process information usage → download and ~~access~~ use of process files.

II. Encrypted process information management: Encrypted process information should be stored in a closed network environment. The devices for downloading and storing encrypted process data must be stationary device. Additionally, the network address is limited to a physical IP address. IP information needs to be recorded in Attachment 1 of the Process Information Usage Application Form and List of User.

III. Application documents: Process Information Usage Application Form and List of User -Encrypted Processes, List of Users (Excel file), TSMC NDA main ~~text~~ document (signing by school representatives), TSMC NDA attachments (signing by professors and authorized users), Encrypted Process Information Protection Statement, Self-Checklist for Encrypted Process Information Management and Supporting Documents.

IV. Information management self-assessment: The Encrypted Processes Information Management Self-assessment Form and relevant supporting documents should be completed and submitted by professors upon submitting their initial application. Subsequently, the Information Management Self-assessment Form and supporting documents must be resubmitted every six months. The deadline for submission will be communicated by TSRI.

V. Information security field audit: TSRI will dispatch personnel to the laboratory to conduct an information security field audit when professors submit their initial application. Subsequently, on an annual basis, the center will conduct on-site audits at laboratories of applying professors through random sampling.

VI. Information security courses: TSRI will dispatch personnel to conduct information security course and examination at the laboratory when professors submit their initial application. The applying professor or assigned administrator, as well as all authorized users, must attend. Subsequently, every year, the applying professor or assigned administrator and all authorized users must participate in the TSRI's e-Learning information security course and examination.

VII. Process information usage authorization: The professor’s team that pass the approval of application documents, information security on-site audit, and information security course and examination are eligible to obtain encrypted process information usage authorization. In principle, the authorization is valid from the process authorization date until December 31 of the respective year.

VIII. Process technical information download system: The professor’s team that has obtained authorization to access encryption process information ~~may~~ can download the applied process information at the TSRI’s technical information download system (TSRI website → chip implementation →Process/Silicon Intellectual Property(SIP)→ technical data download).

IX. Corresponding EDA software/versions: The usage of encryption process files is identical to that of unencrypted process files. However, it is necessary to use the corresponding EDA software, with special attention to matching the same version of Synopsys HSPICE (The TSRI presently offers three versions: 2013.03-SP2, 2015.06, and 2016.03).

X. Chip manufacturing application system: Similar to the general process application Tape-out mode, the professor's team uploads all of the Tape-out application files directly to the TSRI website from the lab's design environment. The tape-out application system: TSRI Website → Chip Implementation → Chip Implementation → Tape-out Application. There is no need to transmit files through the EDA Cloud system.

XI. Destruction of process information: When a professor and/or authorized user stops using or loses the right to use encrypted process information or no longer uses encrypted process information, they must delete all obtained process information. Additionally, they must sign and submit an Encrypted Process Information Destruction Confirmation Form, declaring that all encrypted process information has been immediately and completely delete to prevent any infringement and ensure that it is not disclosed or used by anyone.