**Proposal for FOSS Compliance Processes**

A. Provide technical and organizational equipment for handling FOSS compliantly

1. Repository for managing FOSS
   1. Set up a such repository
   2. Set guidelines for using such repository (function, how to use it)
2. Assign responsibilities
   1. Create the roll of FOSS Compliance Officer
      1. Define the fields you need compliance officers for (i.e. legal, development etc.)
      2. Define the requirements such FOSS Compliance Officer needs to meet
      3. Put someone in charge of FOSS compliance
         1. Assign responsibility to someone within in your company who meets the requirements
         2. Get outside counsel or experts to fulfill the job of FOSS Compliance Officer
      4. Train and educate the FOSS Compliance Officers
         1. legally
         2. technically
      5. Assign staff supporting the FOSS Compliance Officers
         1. Define the requirements such staff needs to meet
         2. train and educate the staff
            1. legally
            2. technically
   2. Resource FOSS Compliance Officers
      1. Develop processes, procedures, templates, forms etc.
      2. Consider using compliance tools
         1. Assess, if you need compliance tools
         2. Define your needs/ requirements for such tools
         3. Evaluate, develop or acquire and deploy tools
         4. Train and educate the FOSS Compliance Officers and/or staff with regard to using such tools

B. Building an entrepreneurial culture regarding the precautions for handling FOSS

1. Trainings/ awareness-programs of programmers/those handling FOSS
   1. Depending on company size
      1. Set up such training/ awareness-program
      2. Enroll in such programs
   2. Content:
      1. Identify FOSS
      2. FOSS concepts and obligations
      3. Relevance of adhering to FOSS license obligations
      4. How to adhere to FOSS approval process
   3. Repeat such trainings/ awareness-programms
   4. Require relevant employees to attend or set up an incentive system for all relevant employees to enroll; relevant employees are:
      1. software developers
      2. software program managers
      3. software procurement roles
   5. Keep track of who enrolled when
2. Lay down guidelines, documentation and FOSS policies for internal use of FOSS in code generation; they need to be
   1. Written
   2. Internally available
   3. Record them
3. Create checklist of what needs to be done when handling FOSS
   1. Written
   2. Internally available
   3. Record them
4. Active contribution to FOSS projects

Build an understanding FOSS licensing and FOSS projects

C. Ensure all necessary information for handling FOSS compliantly is known and reliable

1. Lay down guidelines, documentation and FOSS policies for what FOSS is allowed to come in. Such guidelines need to be:
   1. Written
   2. Internally available
   3. Record them
2. Scan incoming FOSS
   1. Define guidelines for internal scanning
      1. Written
      2. Internally available
      3. Define „incoming FOSS” (download/ developed by employees/ freelancers/ students/ delivered by supplier etc. – What needs to be scanned?)
      4. Define how the scan is to be conducted
      5. Define what keywords are to be searched for.
   2. Conduct such scan:
      1. Adhere to guidelines
      2. Define unit to conduct the scan
         1. Designated unit within the company
         2. External company
   3. Document the outcome of scans you conducted regarding
      1. Applicable licenses including versions
      2. Copyright notices
      3. Source code
   4. Maintain FOSS record
   5. Review applicable licenses
      1. Define guidelines for such review
         1. Written
         2. Internally available
      2. Extract and document license obligations that need to be fulfilled
         1. Assign job to person who is experienced in handling software, especially FOSS licenses
         2. General extraction and documentation for licenses that are commonly applicable to FOSS used (i.e. checklists)
         3. In individual cases

D. Lay down guidelines for suppliers: Define process for software coming in from suppliers

1. Written
2. Make them available to FOSS suppliers
3. Define which FOSS you accept
4. Define what disclosures you expect from your suppliers
5. Define what information/data your suppliers are to deliver with the FOSS
6. Review material delivered by your suppliers
7. Check how your suppliers handle FOSS/ Guidelines for review

E. Set up a review and approval procedure

1. Lay down a FOSS policy
   1. Written
   2. Internally available
   3. Content
      1. Describe FOSS approval process for ensuring that how FOSS is handled in your company is permanently checked
      2. Describe how to utilize it
      3. Which software has to be reviewed and approved
      4. Under which circumstances
      5. Procedures for ensuring all necessary information is available
      6. Procedure how denials of approval are handled
2. Checking that denials of approval are adhered.
3. Checking license compatibility
   1. General guidelines for license compatibility
      1. Which licenses are compatible?
      2. What is the technical design in case of compatibility/ incompatibility (i.e. mixing code, dynamically or statically linking code)
   2. Individually check license compatibility
      1. Define conditions under which such individual check has to be conducted
      2. Check that the procedure is adhered to

F. Ensuring software can be licensed to third parties under FOSS licenses

1. Ensuring all necessary rights are obtained (Enabling FOSS licensing)
   1. (standard) contracts for employees, suppliers, freelancers, students, others containing a clause suffiently transferring and assigning of rights of use
   2. Managing these contracts
   3. Ausreichende Rechteklausel in den Verträgen von Mitarbeitern etc.
2. Ensuring there’s no „accidental FOSS“ (FOSS is not accidentally used in proprietary software.)
   1. Laying down guidelines for contributions of employees etc. in FOSS projects and community contributions (Community engagement is understood)
   2. Written
   3. Internally available
   4. Individual contributions are reviewed and approved
   5. Company contributions are reviewed and approved
   6. Community participation is reviewed and approved.

G. Distribution

1. FOSS policy
   1. Written
   2. Internally available
   3. Define the term „distribution“
2. Ensure license obligations are met/ check outgoing FOSS
   1. Documentation obligations are met
   2. Source code obligations are met
   3. Community interface exists
      1. Email and postal addresses work
      2. Web portal works
      3. Community requests and inquiries are satisfied
3. Ensure such distribution does not happen accidentially, i.e. by co-operation with other companies within your group of company
   1. Fulfill all license requirements irrespective of whether the requirements of a distribution are met
   2. Set up a special legal entity for designated development projects and ensure FOSS is only used within such legal entity