openIDL - Policies

Discussion notes:

Security Policies	SP.01	7/8	A Node Operator MUST maintain and follow IT security policies and practices that are integral to maintain protection of all services provided in association with the openIDL Node Agreement (“Node Services”). These policies MUST be mandatory for all employees of the Node Operator involved with providing the Node Services.	DR - GOVERNANCE POLICIES AND TERMS OF THE PLATFORM - CISOs and CIOs involved, not only loiking at security and data segmentation from T or Hartford and outside rules into that - that might sound non trivial but isnt - inc non standard practices to rules-oriented sec org - big issue or possibly - track compliance - LARGE POSSIBLE COST JB - sec policies will comply with sec reqs of member orgs DR - great in theory but not in practice, everyone has diff reqs, next to impossible to get ONE set all conform to JB - maybe get a set of policies, (sean to pull from recording) DR - more you just say "carrier expose this, figure out how to secure it, audit it" more successful - more you do "here is how you operate" the less successful PA - openIDL network will maintain the security of the stuff in the network and the carrier will secure the data they submit DR - have an auditing platform, if our role is to secure data, answer questions, apply, - deviation will require X - all sep concerns for security maintenance and agree upon some mech for auditing and process acceptance - word it in a more open way JB - things inside and outside network, def do something more of a sep of concerns DR - cant be too prescriptive, trust and process based, leverage well known and well accepted standards JB - participants - some facility that doesn't make it overly complex DR - fits into gov playbook PA - high prob will want to see all data encrypted at REST in HDS - CARRIER REQUIREMENT? DR - zero trust, data will be encrypted at rest KS - Senofi, Chainyard to host nodes for a carrier - who is the node owner ? THing learned early on, tech stack vs security, hosting a node is very diff than on-prem (or on-prem cloud) DR - sep two at this point, nuanced depending on how defined the arch, can work on defs in parallel, too nuanced to lock down now - dep on how we build? KS - delegate all sec concerns to NodeOp, catch-22 idea of what we think is imp, work on arch Ash - Roles here - owner, operator, combining the operations piece and the data pices - fully agree we need to have gov, policies driven by reqs, roles crit in defining, outsource node infa build out, on-prem, cloud, policies and gov - defines what is expected of that role, talk about operator - few rules in there, people doing data loading, cert, stuff, is that KS - Dev ops, diff roles, set of roles about users in the network and people maintaining DR - make it real, have conv in detail - who can consent to a data call - assume the arch puts that in carrier cloud next to HDS, easy - arch really needs to live in node outside of carrier, then define roles differently - dep where we go, very imp pieces of stack in diff locations, dont know how to divvy roles up UNTIL finalize Arch JB - fair, consent to something business decision whereas execution is done by operator DR - maybe 3rd party op role, once finalize arch, define how many and what roles needed PA - do we have a req for data at rest? all stuff encrypt-decrypt all the time KS - assume permissions to run, need a req to make it possible to encrypt DR - for T they will encrypt, thinks all should encrypt at rest, present in way for them to encrypt theirs, what level of anon/agg occurs outside of - we do agg out of their node (not anon yet), if that were to be stored, would like Req that be encrypted - once joined and aggregated, going to be released anyway, but before joining should be encrypted - some in-betwen time where data stored somewhere, if stored should be encrypted PA - where the future is going DR - keys managed by node operator, or by AAIS in node, wherever joined, thats who owns the keys, only one ecrypt and maintained by T and thats HDS JB - request, goes thru mech by each carrier, some mean KS - all these results will land in an analytics node non-anonymized, encrypting only half the problem, unencrypted doesnt stick around in identifiable form for a x amount of time JB - anon from which carrier and then anon of data itself KS - extraction pattern - agree data is stripped of PII DR - agg is data from T but attributable to T - anything attributable needs to be encrypted - good ex: anticpate doing this, like SaaS vendors, no opinion on how they do things but must be encrypt, etc. and proof: DID YOU DO IT? (auditable/provable) - way this will go at each stage

Security Policies	SP.02	7/8	The Node Owner shall designate its CIO, CISO or another officer to provide executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.	
Security Policies	SP.03	7/8	Node Owner shall designate a Security Lead 1 and Security Lead 2 for day-to-day messaging and evaluation of security issues affecting nodes and the network.	
Security Policies	SP.04	7/8	A Node Owner MUST review its IT security policies at least annually and amend such policies as the Node Owner deems reasonable to maintain protection of its Node Owner Services.	
Security Policies	SP.05	7/8	Node Owner MUST maintain and follow its standard mandatory employment verification requirements for all new hires involved with providing its Node Services and will extend such requirements to wholly-owned subsidiaries involved with providing its Node Owner Services (Because Node administrators are a potential threat vector).	
Security Policies	SP.06	7/8	In accordance with the Node Owner's internal process and procedures, these requirements MUST be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by the Node Owner.	
Security Policies	SP.07	7/8	Each Node Owner company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.	
Security Policies	SP.08	7/8	Employees of a Node Owner involved with providing its Node Owner Services MUST complete security and privacy education annually and certify each year that they will comply with the Node Owner's ethical business conduct, confidentiality, security, privacy, and data protection policies. Additional policy and process training MUST be provided to persons granted administrative access to components that are specific to their role within the Node Owner's operation and support of its Node Owner Services.	
Security Policies	SP.09	7/8	If a Node Owner hosts its Node in its own data center, the Node Owner’s security policies MUST also adequately address physical security and entry control according to industry best practices.	
Security Policies	SP.10	7/8	If the Node Owner hosts its Node using a Node Operator (third-party Hosting Provider), the Node Owner MUST ensure that the security, privacy, and data protection policies of the Hosting Provider meet the requirements in this document.	
Security Policies	SP.11	7/8	A Node Owner MUST make available to openIDL, upon request evidence of stated compliance with these policies and any relevant accreditations held by the Node Owner, including certificates, attestations, or reports resulting from accredited third-party audits, such as ISO 27001, SSAE SOC 2, or other industry standards.	
Security Policies	SP.12	7/8	A Node Owner MUST maintain Node Owner keys on a separate machine from the machine that runs their node. This machine, called the “CLI (Command Line Interface) system”, uses Node Owner keys to authorize the Node to participate in the pool, and is thus the basis for trust for the node and the Node Owner’s identity on the network. The CLI system is not required to have high-end hardware, but in terms of IT best practices for security, it must meet or exceed the standards for the Node (see following items). (TBD config specs)	
Security Policies	SP.13	7/8	A Node Owner MUST provide certification that their Node runs in a locked datacenter with appropriate levels of security, including the specifications that they target (e.g., SSAE 16 type II compliance; other standards may also be acceptable). (TBD config specs)	
Security Policies	SP.14	7/8	A Node Owner MUST assert that their Node is isolated from internal systems of a Node Owner (TBD config specs)	

Security Policies	SP.15	7/8	A Node Owner MUST assert that their Node, and its underlying systems, uses state-of-the-art authentication for remote access (at least SSH with key plus password plus source IP firewall rule, and two-factor authentication wherever possible).(TBD config specs)	
Security Policies	SP.16	7/8	A Node Owner MUST NOT allow access (remote or local) to the Node or CLI systems by anyone other than assigned admins.	
Security Policies	SP.17	7/8	A Node Owner MUST apply the latest security patches approved by the TSC within one (1) week or less (24 hours or less is recommended).	
Security Policies	SP.18	7/8	A Node Owner MUST attest that the Node runs on a server protected by a firewall that, at minimum: a. Disallows public ingress except on ports used by the Node software (different machines may choose to expose ledger features on different ports, so no standard port setup is required). b. Optionally enables SSH, Remote Desktop, and similar remote access tools but constrains ingress for these tools in some way that excludes the public but allows access for admins. c. Locks down egress ports to limit the ability to jump from Node to some other location.	
Security Policies	SP.19	7/8	A Node Owner MUST run the Node Owner security check tool as requested, and MUST receive TSC approval of the results before the Node is authorized to participate in consensus.	
Security Policies	SP.20	7/8	A Node Owner MUST run the Node Owner security check tool from time to time as requested by the TSC and provide the test results report to the TSC within three (3) business days.	
Security Policies	SP.21	7/8	Node Owners MUST maintain and follow documented incident response policies consistent with NIST guidelines for computer security incident handling and will comply with data breach notification terms	
Security Policies	SP.22	7/8	Node Owners MUST investigate unauthorized access of which the Node Owner becomes aware (security incident), and the Node Owner will define and execute an appropriate response plan.	
Security Policies	SP.23	7/8	openIDL may notify the Transaction Endorser of a suspected vulnerability or incident by submitting a technical support request.	
Security Policies	SP.24	7/8	Node Owners MUST notify openIDL without undue delay upon confirmation of a security incident that is known or reasonably suspected	
Security Policies	SP.25	7/8	The Node Owner will provide openIDL with the reasonably requested information about such security incident and the status of any of the Node Owner remediation and restoration activities	
Operating Policies	OP.01	7/8	A Node Owner MUST run the most up to date release of the openIDL Open Source Code as approved and designated by the Technical Steering Committee	

Operating Policies	OP.02	7/8	A Node Owner MUST facilitate an upgrade to a new version of the openIDL Open Source Code within three (3) business days of a new release that has been recommended by the openIDL TSC	
Operating Policies	OP.03	7/8	A Node Owner MUST register all Node configuration data (TBD) required by openIDL in a timely manner, keeping information up to date within three (3) business days of changes.	
Operating Policies	OP.04	7/8	A Node Owner MUST have at least two (2) IT-qualified persons assigned to administer the node, and at least one other person that has adequate access and training to administer the Node in an emergency, such as the network being unable to reach consensus or being under attack. See the openIDL Crisis Management Plan (TBD) for details.	
Operating Policies	OP.05	7/8	A Node Owner MUST supply contact info for all administrators to openIDL, whose accuracy is tested at least quarterly (e.g., by sending an email and/or text that doesn't bounce).	
Operating Policies	OP.06	7/8	A Node Owner MUST maintain a system backup or snapshot or image such that recovering the system from failure could be expected to take one hour or less.	
Operating Policies	OP.07	7/8	Node Owner MUST equip at least two (2) technical points of contact responsible for administering the Node Owner Node with an SMS-capable device for alerting.	
Operating Policies	OP.08	7/8	Node Owner SHOULD aim to achieve at least 99.9% (three nines) uptime for their Node (this amounts to about 1.4 minutes of downtime per day or 9 hours per year).	
Operating Policies	OP.09	7/8	SHOULD coordinate downtime with other Node Owners in advance via a mechanism as determined from time to time by agreement between the TSC and any other relevant openIDL Governing Body.	
Technical Policies	TP.01	7/8	Nodes on the openIDL Test Network (testnet) should be similar, but requirements may be downgraded from MUST to SHOULD.	
Technical Policies	TP.02	7/8	Nodes MUST run on robust server-class hardware.	
Technical Policies	TP.03	7/8	If a Node is run on a VM, the Node Owner: a. MUST run on a mainstream hypervisor that receives timely patches from its vendor or community. b. SHOULD apply X patches on a regular basis.	

Technical Policies	TP.04	7/8	The Node MUST run in an OS that is dedicated to the openIDL network, i.e., a single-purpose (physical or virtual) machine that MUST run openIDL Open Source Code, MAY run other software approved by the TSC, and MUST NOT run any other software.	
Technical Policies	TP.05	7/8	Software required to support the node, such as monitoring, backup, and configuration management software, are approved as a general category. However, Node Owners should discuss with the TSC any software packages that transmit between the Node Owner Node and the outside.	
Technical Policies	TP.06	7/8	Nodes MUST run a server with compatible versions of the operating systems supported by the Hyperledger Fabric requirements as documented in the release notes.	
Technical Policies	TP.07	7/8	Nodes MUST have adequate compute power (TBD config specs).	
Technical Policies	TP.08	7/8	Nodes MUST have adequate RAM (TBD config specs).	
Technical Policies	TP.09	7/8	Nodes MUST have at least ((TBD config specs)) 1 TB, with the ability to grow to 2 TB, of reliable (e.g., RAIDed) disk space, with an adequately sized boot partition.	
Technical Policies	TP.10	7/8	Nodes MUST have a high-speed connection to the internet with highly available, redundant pipes (TBD config specs)	
Technical Policies	TP.11	7/8	Nodes MUST have at least one dedicated NIC for openIDL Node consensus traffic, and a different NIC to process external requests. Each NIC must have a stable, static, world-routable IP address. (TBD config specs)	
Technical Policies	TP.12	7/8	Nodes MUST have a system clock that is demonstrably in sync with well-known NTP servers.	
Technical Policies	TP.13	7/8	Nodes SHOULD have a power supply consistent with high availability systems.	

Time	Item	Who	Notes