NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations

Control	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls	Data Collection	Evidence Detail	Finding	Disposition	Threat(s)	Vulnerability Description	Mitigating Factors or Compensatory	Likelihood	Impact	Overall Risk	Risk Explanation
MP-1	Policy and Procedures	Streeting, because, and described in Splagueres agreements of before ground or Splagueres and splagueres and s	Modified presentation parties and presentations and early to the controls in the Set of Monthly that are dispersated in the Set of Set	FM 0, FL 0, 23.2	totenslew	Director of IT, Sich Smith	No media protection policy or procedures were assifable.	Not in Flace	Unauthorized access	No documented processes or politics.	Tribal knowledge in place	5	5	3	Salif do not know what expectations or dendered we and no process around refull professions, sometimes of contractions, shored, see the contraction of contractions in documented on may not be done properly. Without standards and explory results of the contraction of the contract
MP-2	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined paracient or rolles].	System media includes digital and one-digital media. Digital media includes fished drives, dependent processes and sections of the section of	AC-15, AU-9, CP-12, CP-10, MA-5, NP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-14, SP- 12.	Interview	Director of IT, Bob Smith Network Engineer, Tony Jones	USB Drives are not automounted All sensitive data is protected through access controls and database access is logged. DLP solution "name" is implemented and blocking data exist.	In Place						0	CONTROL IN PLACE
MP-3	Media Marking	Mark system media influsing the distribution brothston, harding create, and applicable security melving (if any) of the information, and superior security melving (if any) of the information, and Descript (Assignment: organization-defined types of system media) from meaking if the media remain within (Assignment: organization-defined controlled areas).	Security marking orders to the applications or as of human-residual security articleus. Digital read included disblates, negetict spans, referred or removable had disblates lag, solid reclaim particleus of the control of the disblates lag, solid reclaim pages and microline. Control less control of the disblates and Resconds historisation size with the appropriate subgranting of dissementation requirements for such information and in coefficien in 20 CFR 2022. Security markings are the public disassimal residence of the control of the disblates and Resconds historisation size with the public disassimal residence or regulations are regioner markings for public information industing that the orientation public price size and public pricessals. Security medical security markings are public information industing that the orientation public pricessals is sport medical articleus for effects applicable information industing that the orientation industries public orientation industing that the orientation is public presentation industries that the control of the c	AC-16, CP-9, MP-9, FE-32, 39-32.	Interview	Director of IT, Bob Smith Network Englineer, Tony Jones	Reviewed documentation of identified media for marking (covid data, firancials). Covid data had marking, financial data did not have marking consistently.	Partially in Place	Data Loss/Information Disclosure	Without media marking, financial data could be disseminated to unsubtrared purets. Financial data could accidental be disseminated to unsubtrared parties.	None	2		16	Financial data inn't disclosed often by accident, but when it is its has a negative impact on moral and investor confidence.
MP-4	Media Storage	a Physically control and assured years (hangement: representation defined types of digital and/or the physically control and assured years (Marcia State August the media are desirately of a satisfied using the physical represent, belonges, and procedure.	System and such six factor again and reading state makes. Six for mineral states from the control of the contro	AC 18, CP-3, CP-4, CP-50, NP-7, NP-	Interview	Director of IT, Bob Senith Network Engineer, Tony James	No control or governance around thumb drive usage and storage.	Not in Place	Data Loss/Information Disclosure	Malware could be brought into the environment and insider threat could sheal data.	USB Drive automounts disabled	5	5	В	Loss of IP and introduction of maliciosu sub could introduce massive issues.
MP-5	Media Tomport	s. Protect and article (Papageone's operations defined upon of upon or mobile formation to the control papageone or operations of an article of a strainform of the paper of the paper of the article of article of article of article of article of a strainform of a	System would nevide de glief and stort opplier make. Deglief melle schulde flood from augment, camped fair, in die glief word lief. Sin Legisla melle schulde stort sometim augment, camped fair, and glief word lief. Sin Legisla melle schuld sein sometim and paper. Geroffend erne are speech for which temperatures provide private der provident paper. Geroffend erne are speech to fair spreage private speech and see the speech provident melle and spreage private stort george provinces de propriet and senden somet provide conferentity are drought provinces de private senden senden some service conferentity are drought provinces and the senden service senden some service senden service senden service senden service senden service senden service senden service senden service senden service senden service senden service senden service senden service senden service service service senden service service service senden service service service senden service service service senden service service senden service service senden service service senden	AC7, AC31, CP2, CP3, MP4, MP4, P531, Pc2, SC12, SC13, SC23, SC34	totenslew	Director of T.T. Solo Sovieth Network Engineer, Tony James	we dont allow got to travel with dat, we use cloud stongs and have poll access it from the cloud, anywhen, that is went not for maintenance or regain his sensitive data support before being used.	ls Place						a	CONTROL IN PLACE
MP-6	Media Santzatton	a Settle plaggerent opposition delived system middly, part to disposed, whose or led oppositionated central, or interest for most using frequence operations defined substaclem to be changes and providently, and the control of the disposition of the control of t	get of a spation of integrate related months. The analysis of the control integrate related months. The control integrate related in the control integrated integrates and integrated months of integrates and integrated months of integrates and in	AC-3, AC-7, AU-31, MA-2, MA-3, MA-4, MA-3, TW-22, 39-32, 39-32, 39-32, 39-31	Tested	molewed audit records of HDD destroyed. I was recent, but other I was no destroyed in the I was not in the I was a light of the I was a	Santtaktion is happening, bud incorrelated of documented.	Partisily in Place	Data Loss/Information Disclosure	Without record legging them is no sources of proper sentitations. New people could take over process and result in it not being fone.	Tribal broadedge process and small IT team with one pay that stake in considerity does it.	ž		15	There is no assurance of proper sentiation. This ill insuledge sentiation is the sent of t
MP-7	Media Use	a Judicitius funcio, Probabil the use of Juagement aspertitution defined igns of system medal and Juagement aspertitution defined igns of system medal and Juagement aspertitution defined in the system components are great the system of the	Specimen and excludes both right and one-signal results. Organ in each scalable obtained by the contract of th	AC-18, AC-28, Et-4, PM-12, SC-94, SC-41.	Interview	Director of IT, Bols Smith Network Engineer, Tony Jones	USB Automounting is the only corterol in place. No documented policy or procedures.	In Place						o	CONTROL IN PLACE
MP-8	Media Downgrading	A histabili Jasignment caprination-defined system needs desempeting process) that lectules employing desempting reach assists with trength not integrity commensures with the security category or classification of the information; 3. Merify that they keep media desempting process is commensures with the security category and/or classification level of the information to be removed and the access subnotation of the potential response of the downward information; c. Leferify (Jasignment: agranization-defined system media requiring desempting); and d. Desemption the destination of the commensure and surgit the stability and d. Desemption to destination of the source of the commensure of the source of the d. Desemption of the destination of the disast replaced and process.	Media downgrading applies to digital and non-digital media subject to release outside of the organization, whether the media is considered removable or not. When applied to system media, the downgrading process remova information from the media, high plays years upon a category or dissification lovel, such that the information came be retrieved or reconstructed. Owngrading of media includes medicating information to make whether where are add distribution. Downgrading of media includes medicating information to make whether where are add distribution. Downgrading or make that empty space on the media is devoid of information.	Norse.	Interview	Director of FT, Bob Smith Network Engineer, Tany Janes	There is no process or requirement for media downgrading.	N/A						o	N/A

1 of 2021-01-21